Chapter 1 Introduction 1-1

1.1 Overview 1-1
1.2 Platform 1-1
1.3 Position of the iManager M2000 in TMN Structure 1-2
1.4 System Features 1-4
1.4.1 Main Features 1-4
1.4.2 Basic Features 1-5

Chapter 2 System Architecture 2-1

2.1 Physical Architecture 2-1
2.2 System Hardware 2-2
2.2.1 Hardware Structure of Single-Node Server 2-3
2.2.2 Hardware Structure of Two-Node Cluster Hot Backup Server 2-3
2.2.3 Configuration Requirements for System Hardware 2-4
2.3 System Software 2-6
2.3.1 Software Architecture 2-7
2.3.2 M2000 Server Software 2-7
2.3.3 Data Collection Unit Software 2-12
2.3.4 Client Software 2-12
2.3.5 Intelligent Report System Software 2-13
2.3.6 Configuration Requirements for System Software 2-14
2.4 System Interfaces 2-15

Chapter 3 Services and Functions 3-1

3.1 Configuration Management 3-1
3.1.1 Centralized Configuration Management System 3-2
3.2 Fault and Alarm Management 3-4
3.2.1 Centralized Fault Management System 3-4
3.2.2 iSmsEmail 3-7
3.3 Performance Management 3-8
3.3.1 Centralized Performance Management System 3-8
3.4 Intelligent Report System 3-10
3.5 Common Platform Management 3-14
3.5.1 Topology Management 3-14
3.5.2 Security Management 3-17
3.5.3 Log Management 3-18
3.6 Online Help 3-19
3.7 Remote Maintenance Management 3-19

Chapter 4 Networking Application 4-1

4.1 LAN Mode 4-1

4.2 WAN Mode 4-1

Chapter 5 System Reliability 5-1

5.1 System Protection Mechanism 5-1
5.2 Reliability Measures 5-1
5.2.1 Data Security 5-1
5.2.2 Operation Security 5-2

Chapter 6 System Indices 6-1

6.1 Technical Indices 6-1
6.1.1 Static Value Requirements 6-1
6.1.2 Dynamic Value Requirements 6-2
6.2 Performance Indices 6-4
6.2.1 Server Performance Indices 6-4
6.2.2 System Capacity 6-4
6.2.3 System Operation Environment 6-6

Chapter 7 Specification Compliance 7-1

7.1 Specifications for General Management 7-1
7.2 Specifications for CORBA 7-1
7.3 Specifications for Network Management 7-1

Appendix A Acronyms and Abbreviations A-1

HUAWEI

iManager M2000
Technical Manual

V100R005

iManager M2000
Technical Manual

Manual Version	T2-030212-20040815-C-1.51
Product Version	V100R005
BOM	31025912

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. Please feel free to contact our local office or company headquarters.

Huawei Technologies Co., Ltd.

Address: Administration Building, Huawei Technologies Co., Ltd.,

Bantian, Longgang District, Shenzhen, P. R. China

Postal Code: 518129

Website: http://www.huawei.com

Email: support@huawei.com

Copyright © 2004 Huawei Technologies Co., Ltd.

All Rights Reserved

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks

, HUAWEI, C&C08, EAST8000, HONET, , ViewPoint, INtess, ETS, DMC, TELLIN, InfoLink, Netkey, Quidway, SYNLOCK, Radium, M900/M1800, TELESIGHT, Quidview, Musa, Airbridge, Tellwin, Inmedia, VRP, DOPRA, iTELLIN, HUAWEI OptiX, C&C08 iNET, NETENGINE, OptiX, iSite, U-SYS, iMUSE, OpenEye, Lansway, SmartAX, infoX, TopEng are trademarks of Huawei Technologies Co., Ltd.

All other trademarks mentioned in this manual are the property of their respective holders.

Notice

The information in this manual is subject to change without notice. Every effort has been made in the preparation of this manual to ensure accuracy of the contents, but all statements, information, and recommendations in this manual do not constitute the warranty of any kind, express or implied.

About This Manual

Release Notes

This manual applies to iManager M2000 V100R005.

Related Manuals

The related manuals are listed in the following table.

Manual	Content
iManager M2000 Technical Manual	It introduces the system structure, software functions, hardware functions and networking applications of the iManager M2000 Integrated Network Management System.
iManager M2000 Operation Manual	It is used for assisting the users in GUIs of iManager M2000 Integrated Network Management System.
iManager M2000 Installation Manual	It provides information for the system installation, including the installation of the hardware, server software and client software, and network applications.
iManager M2000 Maintenance Manual	It introduces common problems and troubleshooting in the iManager M2000, as well as the commands of Solaris operating system and Sybase database.
iManager M2000 Intelligent Report System User Manual	It provides an overall introduction to the iManager M2000 Intelligent Report System, including the system architecture, client operation, template customization, software installation, maintenance and examples.

Organization

The manual introduces the system structure, software functions, hardware functions and networking applications of the iManager M2000 Integrated Network Management System.

There are six chapters in the manual.

Chapter 1 Introduction profiles the system characteristics, main features, system platform, and its position in TMN structure of the iManager M2000.

Chapter 2 System Architecture focuses on the system structure, the configuration of hardware and software (including single node and two-node cluster hot backup system)

and external interfaces of the iManager M2000. This chapter describes various software modules of the iManager M2000, including the server software, the data collection unit software, and the client software.

Chapter 3 Services and Functions elaborates on the functions and realization of the system services.

Chapter 4 Networking Application presents the rich networking applications of the iManager M2000.

Chapter 5 System Reliability lists the system protection mechanism and the system measures used in the iManager M2000.

Chapter 6 System Indices lists the technical indices in the iManager M2000.

Chapter 7 Specification Compliance provides the specifications in the manual.

Appendix A Acronyms and Abbreviations lists the acronyms and abbreviations used in the manual.

Intended Audience

The manual is intended for the following readers:

- Technical marketing specialists
- Operation and maintenance personnel

Conventions

The manual uses the following conventions:

I. General conventions

Convention	Description
Arial	Normal paragraphs are in Arial.
Arial Narrow	Warnings, Cautions, Notes and Tips are in Arial Narrow.
Boldface	Headings are in **Boldface**.
`Courier New`	Terminal Display is in `Courier New`.

II. Command conventions

Convention	Description
Boldface	The keywords of a command line are in **Boldface**.

Convention	Description
italic	Command arguments are in *italic*.
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x | y | ...] *	Optional alternative items are grouped in square brackets and separated by vertical bars. Many or none can be selected.

III. GUI conventions

Convention	Description
< >	Button names are inside angle brackets. For example, click the <OK> button.
[ ]	Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forward slashes. For example, [File/Create/Folder].

IV. Keyboard operation

Format	Description
<Key>	Press the key with the key name inside angle brackets. For example, <Enter>, <Tab>, <Backspace>, or <A>.
<Key1+Key2>	Press the keys concurrently. For example, <Ctrl+Alt+A> means the three keys should be pressed concurrently.
<Key1, Key2>	Press the keys in turn. For example, <Alt, A> means the two keys should be pressed in turn.

V. Mouse operation

Action	Description
Click	Press the left button or right button quickly (left button by default).
Double Click	Press the left button twice continuously and quickly.
Drag	Press and hold the left button and drag it to a certain position.

VI. Symbols

Eye-catching symbols are also used in the manual to highlight the points worthy of special attention during the operation. They are defined as follows:

⚠ **Caution**: Means reader be extremely careful during the operation.

🕮 **Note**: Means a complementary description.

Table of Contents

Chapter 1 Introduction 1-1
1.1 Overview 1-1
1.2 Platform 1-1
1.3 Position of the iManager M2000 in TMN Structure 1-2
1.4 System Features 1-4
1.4.1 Main Features 1-4
1.4.2 Basic Features 1-5
Chapter 2 System Architecture 2-1
2.1 Physical Architecture 2-1
2.2 System Hardware 2-2
2.2.1 Hardware Structure of Single-Node Server 2-3
2.2.2 Hardware Structure of Two-Node Cluster Hot Backup Server 2-3
2.2.3 Configuration Requirements for System Hardware 2-4
2.3 System Software 2-6
2.3.1 Software Architecture 2-7
2.3.2 M2000 Server Software 2-7
2.3.3 Data Collection Unit Software 2-12
2.3.4 Client Software 2-12
2.3.5 Intelligent Report System Software 2-13
2.3.6 Configuration Requirements for System Software 2-14
2.4 System Interfaces 2-15
Chapter 3 Services and Functions 3-1
3.1 Configuration Management 3-1
3.1.1 Centralized Configuration Management System 3-2
3.2 Fault and Alarm Management 3-4
3.2.1 Centralized Fault Management System 3-4
3.2.2 iSmsEmail 3-7
3.3 Performance Management 3-8
3.3.1 Centralized Performance Management System 3-8
3.4 Intelligent Report System 3-10
3.5 Common Platform Management 3-14
3.5.1 Topology Management 3-14
3.5.2 Security Management 3-17
3.5.3 Log Management 3-18
3.6 Online Help 3-19
3.7 Remote Maintenance Management 3-19

Chapter 4 Networking Application 4-1
4.1 LAN Mode 4-1
4.2 WAN Mode 4-1
Chapter 5 System Reliability 5-1
5.1 System Protection Mechanism 5-1
5.2 Reliability Measures 5-1
5.2.1 Data Security 5-1
5.2.2 Operation Security 5-2
Chapter 6 System Indices 6-1
6.1 Technical Indices 6-1
6.1.1 Static Value Requirements 6-1
6.1.2 Dynamic Value Requirements 6-2
6.2 Performance Indices 6-4
6.2.1 Server Performance Indices 6-4
6.2.2 System Capacity 6-4
6.2.3 System Operation Environment 6-6
Chapter 7 Specification Compliance 7-1
7.1 Specifications for General Management 7-1
7.2 Specifications for CORBA 7-1
7.3 Specifications for Network Management 7-1
Appendix A Acronyms and Abbreviations A-1

Chapter 1 Introduction

1.1 Overview

The iManager M2000 integrated network management system (INMS) supports the daily operation and maintanence of Huawei CDMA2000 and GSM mobile communication network.

It supports the access to various types of network elements (NEs) listed in Table 1-1.

Table 1-1 NEs supported by the iManager M2000

Type	NE
GSM elements	MSC, HLR, and BSC
CDMA elements	MSC, BSC, BTS, HLR, RAC, and PDSN
GPRS elements	PCU, GGSN, SGSN, and CG

The iManager M2000 also provides the standard common object request broker architecture (CORBA) interface to its upper-level network management (NM) to solve the access problems in the construction of multilevel NM system.

The iManager M2000 enables different operators to implement centralized entire-network management of Huawei mobile communication network.

1.2 Platform

The iManager M2000 runs on a Sun server or workstation with multiple CPUs, internal disk drives, external disk arrays, Ethernet network interface cards, a DVD-ROM, an external robotic tape library, and a UNIX admin workstation.

The iManager M2000 requires ample disk space because it acts as a file transfer protocol (FTP) server and a storage area for the configuration database, history alarm, performance task result, performance item information, and backup files. An internal tape drive is available on some configuration models. The operating system for the iManager M2000 is Solaris 8.

The hardware configuration of the iManager M2000 depends on the size of the managed network. It is possible to size up the hardware.

For the detailed information about the M2000 platform, see Chapter 2.2 “System Hardware”.

1.3 Position of the iManager M2000 in TMN Structure

As the mobile network is developing continuously in scale and complexity, network management is now playing a crucial role in improving network service quality, streamlining the network resource and lowering the maintenance cost. Therefore, a management system with comprehensive functions and in compliance with unified standards is of profound significance to the service quality and maintenance cost of mobile network.

The iManager M2000 is a product in Huawei-developed iManager family, providing mobile network solution. As a NE level management system, the iManager M2000 is located in the NE management layer (EML) in telecommunications management network (TMN) structure. It exercises management over large-scale mobile networks by managing its lower-level sub network management system. The position of the iManager M2000 in TMN structure is shown in Figure 1-1.

Note:

[Telecommunications Management Network TMN]

Telecommunications management network (TMN) is a concept defined in 1988 by International Telecommunication Union--Telecommunication Standard Sector (ITU-T).

TMN serves to provide an organized architecture and standardized interfaces from the perspective of global telecommunication network so that management information can be exchanged in a unified manner between different management systems, between management system and telecommunication equipment, and that the whole telecommunications network can be maintained and managed in an integrated and standard manner.

The management functions in TMN fall into five logic levels: NE level (NEL), element management level (EML), network management level (NML), service management level (SML) and business management level (BML).

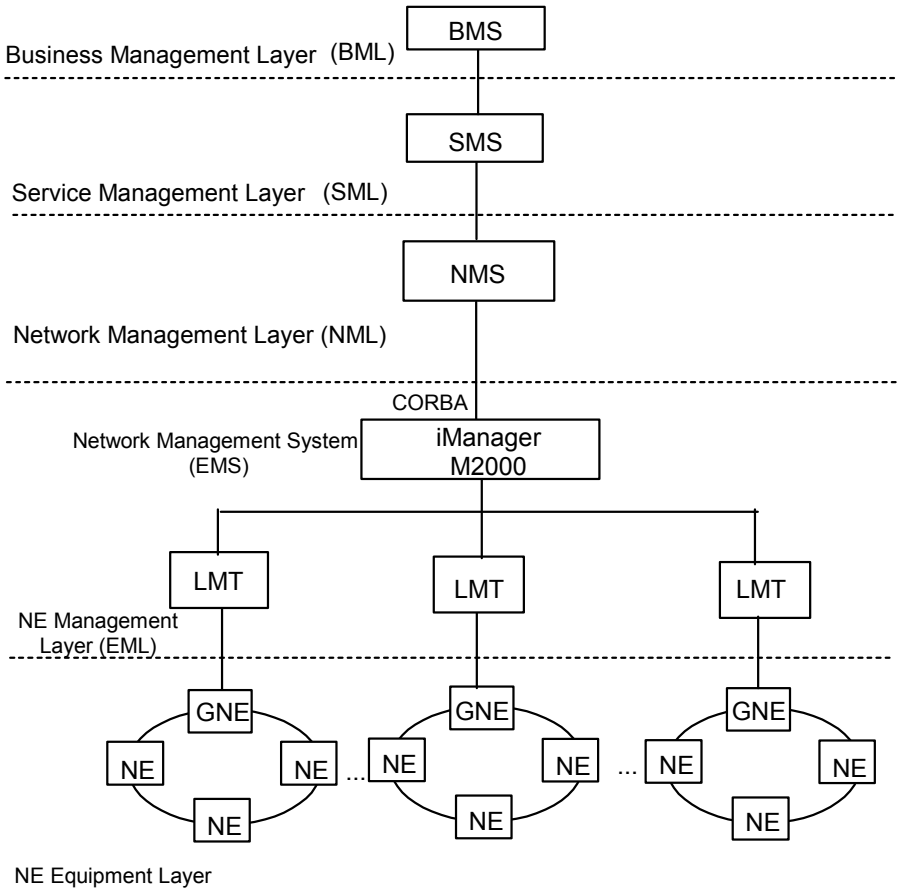


Figure 1-1 Position of the iManager M2000 in TMN

The iManager M2000 performs management over Huawei-developed mobile equipment and network. As the element management system (EMS), the iManager M2000 provides the filtered and abstracted management information for high level network management center (NMC).

Note:

- [EMS]

EMS is responsible for direct management over specific mobile equipment in the mobile network and for information exchange with the upper-level network management system. EMS is the lower-level network management system of the network level management system.

Huawei-developed NE LMT is sub-network management system in the mobile network.

- [CORBA Interface]

CORBA interface is the interface between Manager and Agent in TMN. It includes not only open systems interconnection (OSI) communication protocols from layer 1 to layer 7 but also management message and management information base (MIB) in layer 7.

1.4 System Features

The iManager M2000 system is a feature-rich system. The following details its main features and basic features.

1.4.1 Main Features

The iManager M2000 system is highlighted for the following features:

- It provides software and hardware networking solutions of different costs according to different network operation and management requirements.
- Multiple physical transmission methods, such as E1, T1, X.25 and DDN, can be used to implement flexible system networking.
- The modular design enables the smooth expansion of the system. The access of NE can be realized by directly adding topology and configuration data. When the network grows to a certain scale, the smooth expansion of the system can be implemented by adding servers to share the load.
- The system provides standard CORBA interface to the upper level network management system, and secondary development interfaces for third-party software.
- The system provides forwarding alarm function. The alarms can be forwarded to specified users through wireless Modem or Email, in short message or Email mode.

1.4.2 Basic Features

I. Configuration Management

Through the Internet Explorer, the centralized configuration management function can:

- Control the configuration information of the entire network in the centralized mode.
- Directly show the configuration information and navigation information.
- Provide configuration query and browsing, graphical display of frames and boards, as well as the configuration data statistics reports.

II. Fault Management

The centralized fault management function can:

- Display the operation status of the entire network.
- Provide functions such as real-time alarm indication, alarm acknowledge/de-acknowledge, alarm shielding, alarm dispatching list distribution, alarm relativity analysis and alarm query.

Among these, the alarm relativity analysis can reduce the reports of redundant alarm information, so that the maintenance personnel can locate the fault quickly and accurately.

III. Performance Management

The centralized performance management provides the following functions:

- Provide the operation performance data of the network equipment, including the performance item management and graphical display of data.
- Allow setting of the performance alarm.
- Provide other useful functions like statistics, summing up and conditional query of the measurement results.

IV. Topology Management

Topology management offers the following functions:

- Support the functions of vector map zooming and accurate NE locating.
- Provide theme maps to display the alarm and performance information of the equipment on the real-time basis.
- Display the alarm status of individual NEs and links on the real-time basis through NE icon alarm indicators and the link color change.

V. Local Manitenance

Centralized user interface tracing provides functions such as subscriber tracing, interface tracing and signaling tracing.

VI. Intelligent Report Management

The system provides powerful intelligent report tool which allows users to customize the report design. Besides, it provides several performance and configuration report templates. Several report output modes are available so that users can obtain the system data for various operations and maintenance.

VII. Security Management

The system features high security.

In the system, flexible management of the user authority can be implemented by means of dividing NEs into subnets, setting the entire-network manager, subnet manager, entire-network/subnet ordinary users.

Illegal intrusion to the network can be avoided through the ID authentication upon user login and logout.

Meanwhile, to enhance the data security, the system also provides the data backup and restoration functions, and encrypts the data before transmission.

The system can monitor the login users and display the status of each user in the real-time log.

VIII. Remote Maintenance Management

The system supports the dial-up access through Modem to the M2000 server to perform remote maintenance and monitor the remote maintenance on the real-time basis. It also keeps a detailed remote maintenance log. Illegal user can be kicked out from the system. After the remote maintenance, a report will be generated.

Chapter 2 System Architecture

According to the structural characteristics of the mobile network, the functions of the iManager M2000 are implemented in the principle of centralized management and centralized maintenance.

Each equipment entity (such as MSC, HLR, and BSC) is used as a managed element of the iManager M2000 system, and each managed element connects to the iManager M2000 system through the data collection unit (the Adapter).

2.1 Physical Architecture

The iManager M2000 NM is composed of M2000 server, data collection unit (Adapter), operation terminal, dial-up server supporting remote maintenance and the network connection among them. The physical architecture is shown as Figure 2-1.

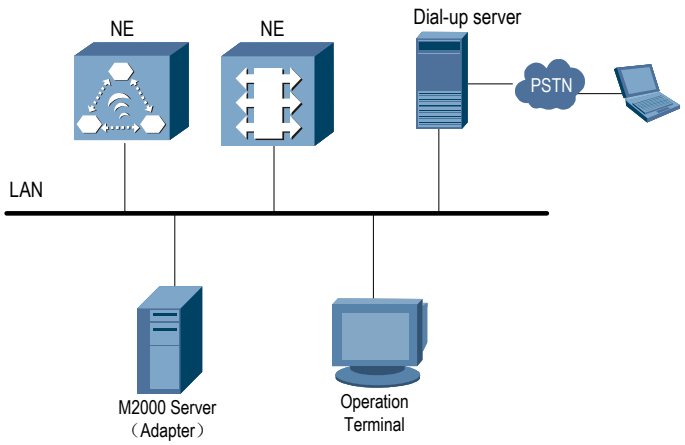


Figure 2-1 Physical Structure Schematic Drawing

The following describes functions of main parts.

I. M2000 Server

The M2000 server is a working station running the Sun Solaris operating system. This server is stored with network configuration data, user data, alarm data, and traffic measurement report data. Sybase is used as its database platform. The number of servers can be configured according to the system capacity.

II. Adapter (Data Collection Unit)

The Adapter is the protocol adaptation module of all NE equipment and provides the basic data on the unified standard for the iManager M2000 system. At the same time, it converts user's network service operation into specific operation commands of individual NEs and submits them to the host for implementation.

Besides, the Adapter is the communication bridge between the iManager M2000 system and NE equipment. Different types of NE correspond to different data collection units.

The Adapter's logic location is between the M2000 server and the managed NE BAM. Its software can be run on an independent physical computer, or on the same physical computer together with the server software. Its selection principle is that the computer performance must meet the system requirement.

Generally, we run the Adapter software and the M2000 server software on the same computer to reduce hardware investment and network nodes, lower network complexity, and make maintenance easier.

III. Operation Terminal

The iManager M2000 operation terminal is the direct interface to perform the O&M management of mobile equipment. It is a computer running the Windows operation system.

The software run on it includes:

- The integrated network management system (INMS).

  The INMS, adopting the geographical information system (GIS), supports electronic map scaling to physically locate NEs in precision, and supports multi-layer display, including visual display of major alarms and configuration data, at the same time.
- The system programs of all application consoles, including the centralized configuration console, the centralized performance console, and the centralized alarm console.
- The local maintenance terminal (LMT) of individual NE itself.

  Relying on LMT, users can complete all operations on NEs managed by the iManager M2000 system. All O&M can be performed on a workstation (WS). The number of the WS can be flexibly configured according to the capacity of the system.

2.2 System Hardware

The configuration of the iManager M2000 system hardware includes:

- Server hardware
- O&M terminals (WS)

The M2000 server is configured in single-server mode or two-node cluster hot backup server. User can select from the following configurations according to the number of the connected NEs in actual configurations.

2.2.1 Hardware Structure of Single-Node Server

With single-node server, the hardware structure of the iManager M2000 is as shown in Figure 2-2.

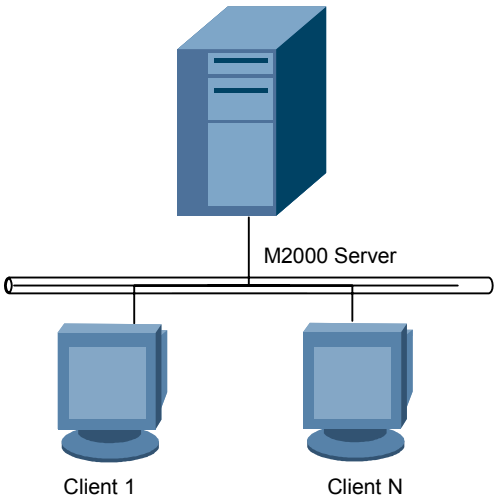
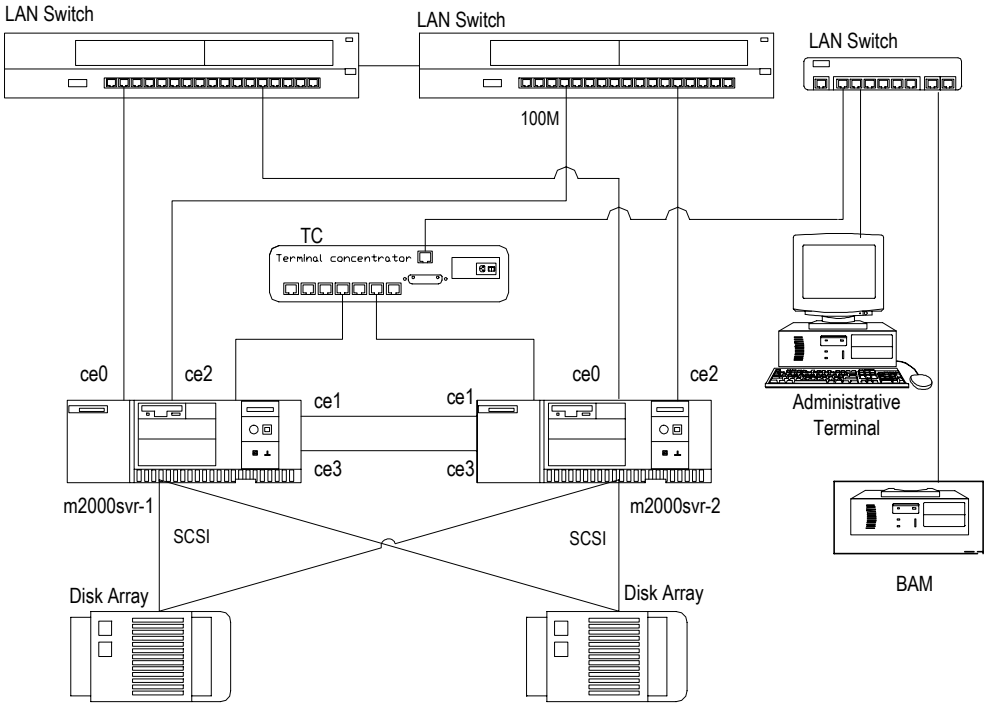


Figure 2-2 Schematic diagram of the iManager M2000 hardware structure (single-node server)

2.2.2 Hardware Structure of Two-Node Cluster Hot Backup Server

To ensure better reliability, the hardware at the server of the iManager M2000 can adopt two-node cluster hot backup mode.

The hardware structure of the two-node cluster hot backup is shown in Figure 2-3. Two servers are both connected directly and through the network (connected with two LAN Switches.).



m2000svr-1	The primary server
m2000svr-2	The secondary server
ce0/ce2	Two network interfaces, connected with public network
Administrative Terminal	The terminal monitoring the server running status
ce1/ce3	Two network interfaces, connected with private network
TC	The terminal controlling the two-node local cluster running

Figure 2-3 Schematic diagram of the iManager M2000 hardware structure (the two-node cluster hot backup server)

Note:

The name of network interface will change with the actual type of network cards.

2.2.3 Configuration Requirements for System Hardware

I. Hardware Configuration Requirements of Client

Configuration requirements for hardware at client are as shown in Table 2-1.

Table 2-1 Recommendations for hardware configurations of clients

	Recommended configuration
CPU	P4 2.4 GHz or higher
Memory	256 MB

	Recommended configuration
Hard disk	40 GB (7200RPM)
Operating system	Win2000 Professional / Win98
Accessories	Floppy disk drive
	CD-ROM
	Integrated netwrork adapter – Integrated audio adapter
	1702FP 17" flat monitor

II. Hardware Configuration Requirements of Server

Table 2-2 provides the hardware configuration recommendations for single-node server.

Table 2-2 Configuration recommendation for single-node server

Configuration / Level / Recommended configuration	Low level	Medium level	High level	Super level
Number of managed NEs	1 – 5	1 – 15	16 – 30	<40
Sun server	Sun Blade 150 CPU: 650 MHz Memory: 1 GB Hard disk: 2*40 GB Dimension: H118×W447×D446mm (H4.65xW17.6xD17.56 in.) Weight: < 15.5 kg (34.2 lb)	Sun Netra20 CPU: 2x1.2 GHz (8M Cache) Memory: 4 GB Hard disk: 2*73 GB Dimension: H177×W435×D496mm (H6.97xW17.1xD19.53 in.) Weight: < 27.3 kg (60.2 lb)	Sun Fire V880 CPU: 1.2GHz × 4 Memory: 8 GB Hard disk: 73GB × 2 Disk array: 3310 (8×36 GB) Tape: DDS4 Dimension: H714×W480×D826 mm (H28.11xW18.9xD32.5 in.) Weight: < 130.9 kg (288.6 lb)	Sun F4800 CPU: 4*1.2 GHz Memory: 16 GB Hard disk: 36 GB × 2 Disk array: 2*T3 (9*36 GB) Dimension: H762×W446 ×D724 mm (H30xW17.56xD28.5 in.) Weight: <131.1 kg (289.1 lb)

Table 2-3 provides hardware configuration recommendations for two-node cluster hot backup server.

Table 2-3 Configuration recommendations for two-node cluster hot backup server

Network status / Recommended configuration	Primary/Secondary servers	Shared Management Terminal	Hub
Sun Server	Sun Netra20 CPU: 1.2 GB x 2 Memory: 4 GB Hard disk: 36GB x 2 Disk array: 2x3310 (5x36 GB) Tape: DDS4	Sun Blade 150 CPU: 650 MHz Memory: 512 MB Hard disk: 40 GB	Quidway S3026 x 3
	Sun Fire V880 CPU: 1.2 GHz × 4 Memory: 8 GB Hard disk: 73 GB × 2 Disk array: 2x3310 (8x36 GB) Tape: DDS4	Sun Blade 150 CPU: 650 MHz Memory: 512 MB Hard disk: 40 GB	Quidway S3026 x 3
	Sun F4800 CPU: 1.2 GB x 4 Memory: 16 GB Hard disk: 36 GB x 2 Disk array: 2xT3 (9x36 GB) Tape: DDS4	Sun Blade 150 CPU: 650 MHz Memory: 512 MB Hard disk: 40 GB	Quidway S3026 x 3

2.3 System Software

The iManager M2000 system software can be logically divided into three parts:

- M2000 server software
- Data collection unit software
- O&M service program (including centralized application console and local application console).

This section introduces the architecture of the iManager M2000 system software and functions of each part.

2.3.1 Software Architecture

It adopts the Client/Server system structure.

TCP/IP is adopted for the communication between different parts.

Figure 2-4 shows the software architecture of the iManager M2000.

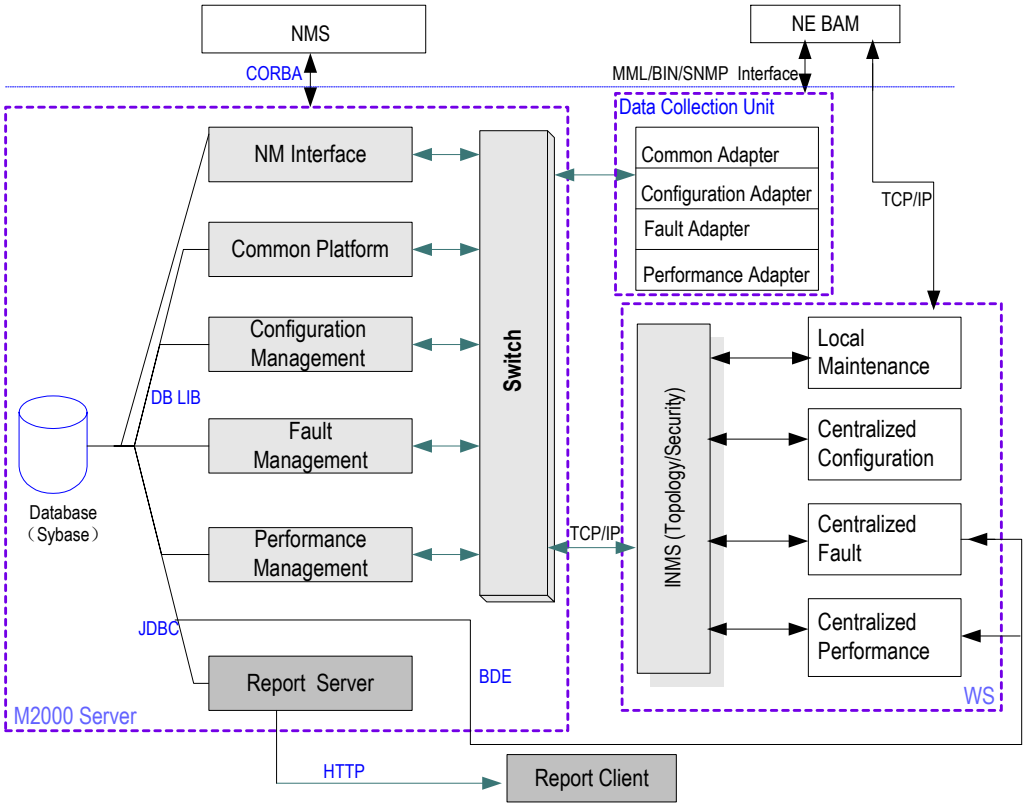


Figure 2-4 The iManager M2000 software structure

2.3.2 M2000 Server Software

M2000 server software includes the follows, and it provides centralized data storage and management:

- Common platform module (security management and topology management.)
- Configuration management module
- Fault management module
- Performance management module
- Intelligent report system

The M2000 server realizes functions of all application servers and NM interfaces of the iManager M2000. They form a group of mutually independent processes.

The intelligent report system is a completely stand-alone system, where the authority and files can be administered, and the report creation for the service database can be conducted by accessing the service database. Its software will be described solely.

I. Common Platform Module

The common platform module involves the switch of M2000 server, security management, log and scheduled task management; integrated network management system (INMS), and the interaction among common modules of data collecting units (Adapter).

- On one hand, the Switch is the mediator for communications among all server modules, INMS and the Adapter; and on the other hand, thanks to its existence, the modularization of the entire iManager M2000 system is realized, namely, all M2000 servers are not restricted by physical locations.
- The security management system, which guarantees the safety of network operation, is an important item of the system performance measurement. Security management includes such functions as safety detection, safety control and alarms. The safety detection function is to detect and count events of breaching safety mechanism. The safety control function is to provide mechanisms to guarantee network safety, such as authentication, encryption, and so on. While the alarm function is to report all actions against security management to the security manager.
- Log is the record of operations on the system. It ensures that important operations (such as user login, adding nodes, and adding users) are recorded, and provides a convenient query mechanism to users. Scheduled task management is to regularly trigger common, configuration, alarm and performance tasks according to the setting of users.
- Integrated network management system is the gateway leading to M2000 O&M. On one hand, it establishes connection with the Switch to realize the system's security management and topology management; on the other hand, it dynamically establishes independent TCP/IP connections with all NEs to realize the local maintenance according to user requirements.
- The common module of data collecting units shoulders such functions as bottom-layer communication, information receiving and transmission, as well as dispatching.

II. Configuration Management Module

Figure 2-5 shows the structure of configuration management module.

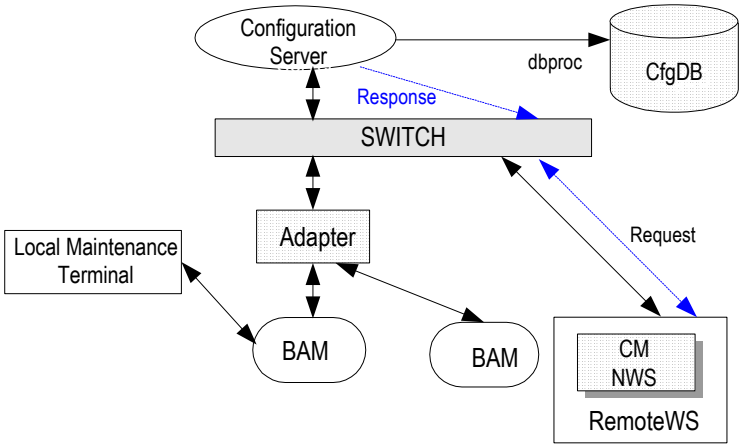


Figure 2-5 Structure of configuration management module

The configuration management module adopts centralized data management to collect data of all NEs in the network, and submit them to users through the graphical mode, so as to provide operations on the NE equipment data. At the same time, the system also provides an open database interface for the upper level NM to access.

The configuration management module is composed of three parts: configuration server, configuration Adapter, and configuration client (CM NWS).

- The configuration server

  The configuration server gets the object tree of the entire system through the configuration Adapter, and saves it in the configuration database for the configuration application console and other servers to perform object and attribute query. Besides, it accepts requests to add, delete or modify topology nodes, and adds, deletes and modifies the corresponding topology data in the configuration database.

- The configuration Adapter

  The configuration Adapter collects data from NE equipment through the interface protocol provided by NE equipment, analyzes collected data according to the object information model, and updates data in the server through the interface protocol provided by the configuration server.

- CM NWS

  CM NWS provides a GUI to realize a series of functions, such as browsing configuration data, browsing scheduled tasks, querying log, and so on.

III. Fault Management Module

Figure 2-6 shows the structure of fault management module.

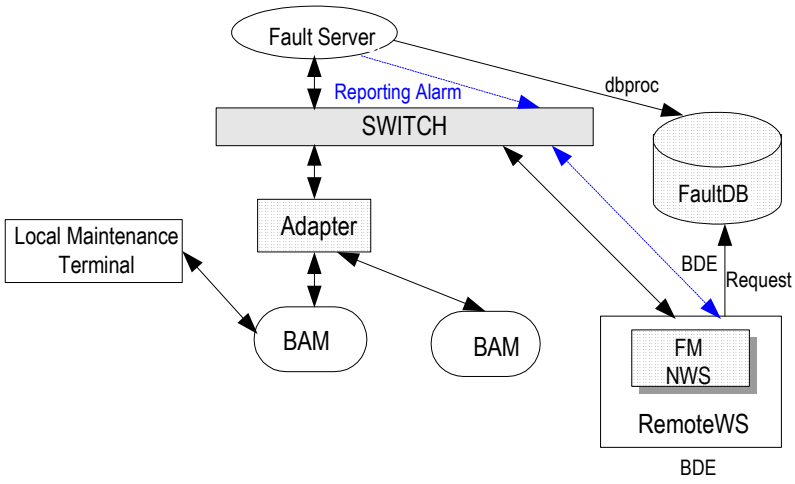


Figure 2-6 Structure of fault management module

The fault management module is composed of three parts: fault server, fault Adapter, and fault Client (FM NWS). Among them, the fault Adapter can be divided into five sub-modules respectively for alarm collection, alarm conversion, alarm repetition filtering, alarm queue, and alarm reporting.

- Fault Server

  The fault server is responsible for the centralized storage management of the alarm data in the entire network. It occupies the core position.

- Fault Adapter
  - Alarm Collection Module

    This module collects alarms generated by equipment. Those alarms can be divided into three types as fault alarm, recovery alarm and event alarm.

    The alarm collection module reports alarms to the BAM in three modes: sending fault alarm query command to the BAM, sending history alarm query command to the BAM, and receiving BAM-generated alarms on the real-time basis.

    Generally, if this module is in normal connection with the alarm server and the BAM, it receives BAM-generated alarms on the real-time basis; if its connection with the alarm server or the BAM is abnormal, alarms generated by the BAM may be lost.

    In order to collect lost alarms after the connection status restores to normal, this module will send a history alarm query command to the BAM to query alarms generated during the specified time segment. Besides, in order to guarantee the alarm information consistency, it regularly sends alarm query commands to the BAM to check current active alarms of the BAM, then

compares alarms of the alarm server and takes corresponding handling measures to inconsistent ones.

– Alarm Conversion Module

Because the iManager M2000 system can be accessed to different equipment, alarm data generated by individual equipment BAMs have their own specific formats. Different BAM determines different alarm data format. The task of the alarm conversion module is to convert BAM-generated alarm data into the format required by the fault server.

– Alarm Repetition Filtering Module

Alarm Repetition Filtering Module checks the repeated data records and repeated data to avoid repeated data reporting. The repeated data record function refers to recording data already reported to the alarm server successfully so as to perform repetitiveness detection on later alarm data. The repeated data detection function refers to detecting data to be reported. If a datum is found reported already, it will be discarded and logged.

– Alarm Queue Module

The alarm queue is a buffer used to store and manage alarm records to be sent. After sending one group of alarm records to the server, Adapter cannot send the next group before it gets receiving response from the server. During the period waiting for response, all waiting alarm records to be sent are stored in the alarm queue.

– Alarm Reporting Module

This module is responsible for reporting alarm records in the alarm queue to the server.

- FM NWS

The FM NWS is an alarm Client terminal with a graphic operation interface. With the visual interface support, users can complete friendly interaction with the fault management module.

IV. Performance Management Module

The structure of performance management module is the same as that of fault management module.

The performance management module provides a visual and complete operation environment for users to implement the system performance management. By collecting various statistics data, it monitors the status and location faults of the network, network units or equipment, performs assessment on the communication equipment status and the network or network unit efficiency, so as to provide reference for network optimization.

The performance management module contains three parts: performance server, performance Adapter, and performance client (PM NWS).

- Performance server plays a key role in the entire performance management system. It distributes the service instructions to each NE, creates task table, analyze the items and save the performance data to the database when registering a task.
- The performance Adapter is used to shield the difference between various network elements, convert special attributes of individual NEs into the standard mode to complete the interconnection between different NEs, and thus to implement the delivery of performance data collection tasks and the reporting of performance data.
- The PM NWS is a graphic interface between the performance management module and the user. It carries out such functions as originating and modifying performance data collection tasks, querying and displaying performance data, and so on.

2.3.3 Data Collection Unit Software

Located between the server and the BAM, the data collection unit (Adapter) implements protocol conversion and service processing, and screens the interface difference between NEs and the network.

Operating on the M2000 server, the Adapter software provides the unified data format for the iManager M2000 system, and converts the user's operations to specific operation commands for various NEs and submits them to the host for execution.

2.3.4 Client Software

The Client software includes the integrated NM system (INMS), configuration management system (CM NWS), fault management system (FM NWS), performance management system (PM NWS) and various NE service maintenance programs.

On one hand, the Client software integrates local terminals, so that all local maintenance functions of NE can be implemented on the Client.

On the other hand, it provides centralized processing capability, including topology management, security management, fault management, performance management and configuration management.

INMS provides the O&M function (including security management, topology management, and startup of service programs), and various centralized management of the local consoles. It can establish the TCP/IP connection directly with the BAM to implement the local maintenance of the NE BAM.

2.3.5 Intelligent Report System Software

The intelligent report system software can be divided into three parts, the report client, the report server, and database proxy server. These three parts coordinately access the service database opened by the service system.

Figure 2-7 shows the architecture of the system.

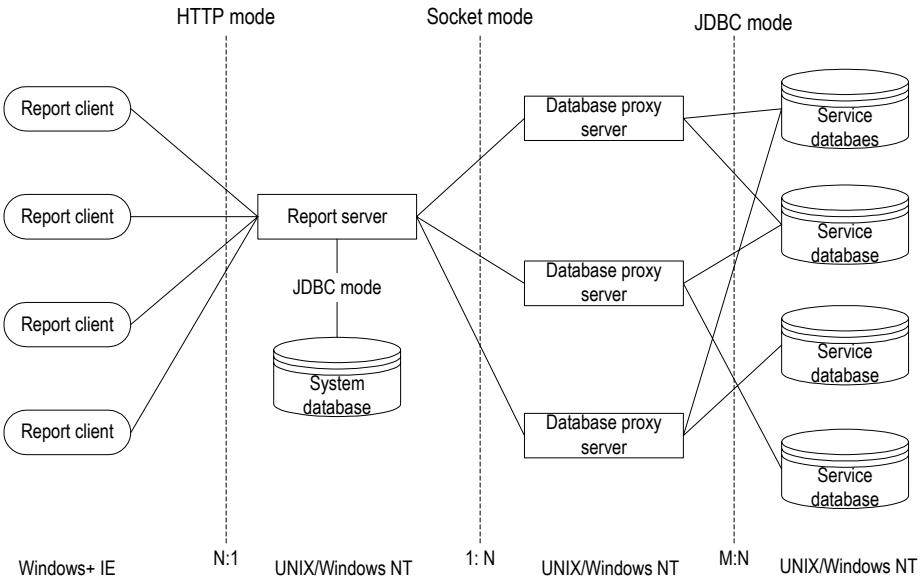


Figure 2-7 Architecture of the report system

Only a report server is allowed in the report system, whereas multiple report clients in the system.

The report server establishes the licensing mechanism. The number of the clients connected to the report server cannot exceed to the number of Licenses. Multiple database proxy servers are available here. Each database proxy server is permitted to access multiple service databases, that is, each service database can be accessed by multiple database proxy servers.

The functions of the main components are as follows:

I. Report Client

The report client is composed of the following elements:

- Client management program

  The client management program includes the user, data source, database proxy server, report and report template of the management system.

- Report template designer

A user can use the report template designer to design a report template file.

- Report query condition setting Interface

  You can set the query condition for a report in the report query condition setting interface.

- Report template browser

  You can use the report template browser to view the report generated in the report system.

II. Report Server

The report server is composed of the following elements:

- Support software: JAVA SDK (1.3.0 or higher)
- System management software

  The system management software deals with the commands sent from the client management program and report designer to the report server, such as login, modifying the data source and downloading the report file.

- Data query software

  The data query software receives the data query request from the client, communicates with the database proxy server to fetch the result, and returns it to the client.

III. Database Proxy Server

The database proxy server can only implement the single function of accessing the database and fetch the query result.

IV. System Database

The system database stores the information of the report system, including the user and authority information, definition of the data dictionary, template file material and other relevant information. The system database adopts the large relationship database, such as Informix, Oracle, SQL Server, and Sybase. The report system database provides a working platform for the report server.

V. Service Database

The service database is the business data source of report system.

2.3.6 Configuration Requirements for System Software

Table 2-4 provides the software configuration of the M2000 system.

Table 2-4 Software Configuration

Category	Software	
Server	Single-node server	Two-node cluster hot backup server
	Solaris 2.8 Sybase Adaptive Server 11.9.X for Sun Solaris The iManager M2000 server application software The iManager M2000 CORBA Agent software (optional) Intelligent Report System software(optional) Volume Manager 3.2 or higher (optional)	Solaris 2.8 × 2 Sybase Adaptive Server 11.9.X for Sun Solaris. Volume Manager 3.2 or higher × 2 SC3.0 × 2 The iManager M2000 server application software × 2 The iManager M2000 CORBA Agent software × 2 (optional) Intelligent Report System software × 2(optional)
Client	The iManager M2000 client software System software: Windows 2000 Professional or Windows 98	

2.4 System Interfaces

I. CORBA Interface

It is a bridge between the NE management layer (EML) and the NML. Following the 3GPP/3GPPII OAM standard, the system can access the third party's integrated NM system through the highly-recommended CORBA interface.

The CORBA interface of the iManager M2000 complies with OMG CORBA 2.5 specifications, adopts IIOP1.2 protocol, and uses standard CORBA Naming Service1.1 and Notification Service1.0.

II. MML Interface

The MML interface is adopted for the MSC/SSP/IP, and SGSN to access the iManager M2000, so as to implement the centralized operation and maintenance.

III. Message/File Mode Interface

The iManager M2000 also opens message/file mode interfaces to the upper-level NM system. The specific interfaces opened are:

- The Sybase database interface provided by the centralized configuration module and the centralized performance module to the upper-level NM system;

- The third party alarm interface provided by the centralized alarm module to the upper-level NM system.

IV. BIN Interface

The BIN interface mode is adopted for the MSC/SSP/IP, HLR, and BSC to access the iManager M2000, so as to implement the centralized operation and maintenance.

V. SNMP Interface

The combined BIN and SNMP interface are adopted for the PCU and GGSN to access the iManager M2000, so as to implement the centralized operation and maintenance.

Chapter 3 Services and Functions

The iManager M2000 provides centralized management services for a mobile communication network. As the core of network system operations, the iManager M2000 plays a key role in all phases of the system life cycle, including:

- Configuration management
- Fault management
- Performance management
- Topology management
- Security management
- Log management
- Online help
- Remote maintenance management

Once the system is handling traffic after commissioning, the iManager M2000 can be used to perform daily and periodic operation tasks designed to keep the network running effectively. These tasks include:

- Monitoring alarms
- Optimizing the system
- Monitoring call performance
- Collecting performance data for off-line analysis
- Implementing backup

3.1 Configuration Management

The iManager M2000 provides GUIs that simplify network configuration and the configuration of individual resources. It supports the following configuration management functions:

- Simply configuring the managed object.
- Synchronizing M2000 configuration data with network element resources.

  When the NE configuration data is changed, the iManager M2000 system will be automatically notified. The M2000 system will collect configuration data once again, and update the configuration tree to keep consistent with the NE configuration data.

The [Configuration Management System] window is the central user interface for network configuration, as shown in Figure 3-1.

3.1.1 Centralized Configuration Management System

The centralized configuration management system of M2000 provides basic resource data for the entire M2000 system with a unified access mode to the resource of the whole network.

The [Configuration Management System] window is shown in Figure 3-1.

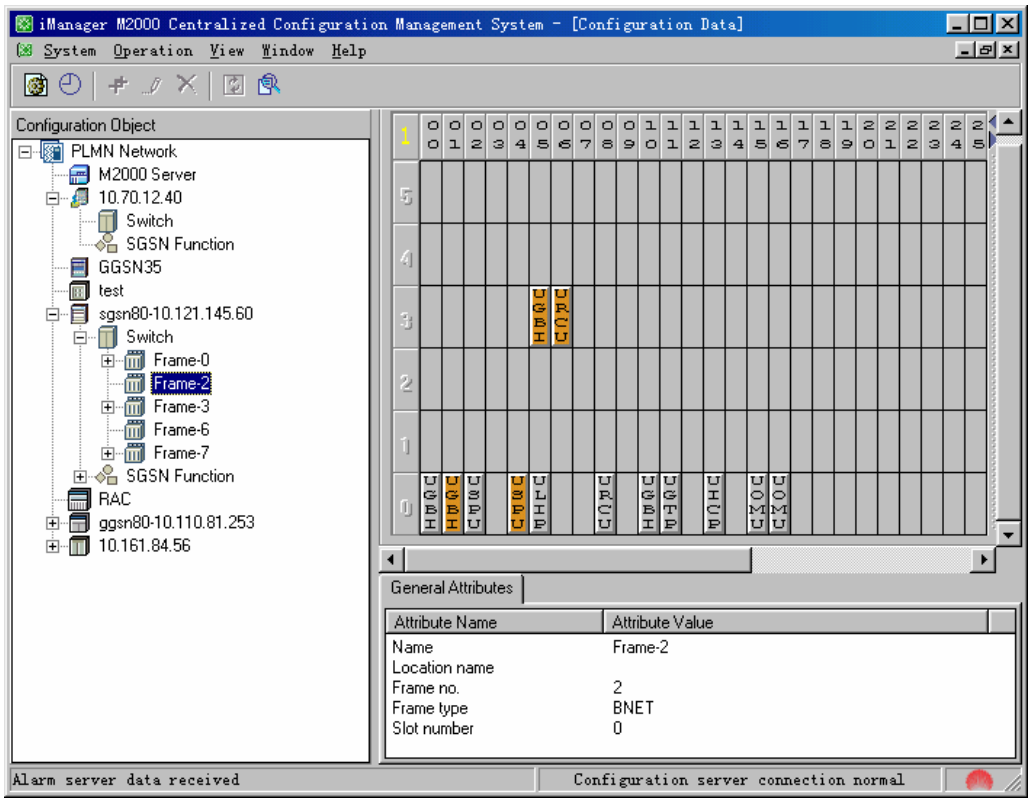


Figure 3-1 iManager M2000 centralized configuration management system window

In this window, the configuration management system provides:

- NE configuration tree

  The configuration management system provides the configuration tree of accessed NEs, as shown in Figure 3-2. This configuration tree displays the relations among all NE configuration data in a tree mode, and the Contained Objects and Related Objects in a centralized mode.

  The configuration management system performs separated management of the physical equipment and logic functions to meet the requirements of performance and alarm services. For example: the speech board and the speech function are treated as different managed objects.

  The NE configuration tree is designed according to the ITU-T standard.

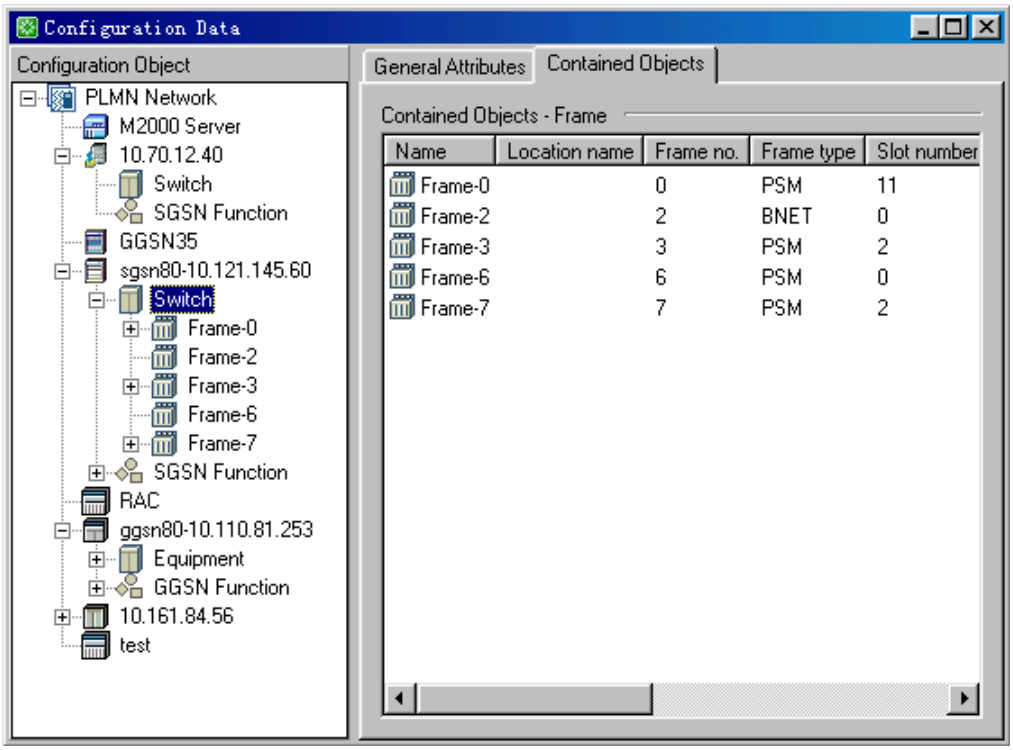


Figure 3-2 NE configuration tree

- Configuration data browsing

  You can browse all the configuration data and the relations among the configuration data with the help of the configuration tree.

  You can also choose to display the required attributes of an object and screen the unrelated ones.

  When you browse the information of an object, the system also displays the related information of other objects at the same time, and graphically displays the objects such as frames and boards. By this way, you can browse the board alarm status timely.

  You can also sort the data of the same type by setting sequencing conditions.

- Graphical display of frame and board

  The configuration data of frames and boards can be displayed according to their type and properties.

  Meanwhile, alarms on frames and boards can be shown in different color.

- Configuration data query

  You can query the configuration information of any NE by specifying the query conditions, and locate the object in the configuration tree.

- Configuration data backup

A scheduled task can be created and automatically implemented every month to backup the configuration data of the NE in the current month. You can also manually backup the configuration data of current NE.

- Scheduled task management

  The scheduled task management module can refresh NE configuration data automatically and backup the data on a scheduled basis. It also performs centralized management and execution of the scheduled tasks.

- Providing configuration reports

  According to the collected configuration data, the intelligent report system can generate the corresponding reports in the format of the report template.

3.2 Fault and Alarm Management

The iManager M2000 fault and alarm management module acts as a gateway to the common fault management application at the NMS. By default, the iManager M2000 subscribes to all fault notifications generated by itself and network elements (MSCs, BSCs, and so on) in its managed area. However, you can halt fault supervision of a specific network element, if desired. As the iManager M2000 receives each fault, it displays the fault as an alarm of a designated severity in an easy to use GUI where the operator can view, acknowledge, and comment on the alarm.

The fault management system comprises:

- Alarm consistency check

  According to the current active fault alarm, the system performs periodic consistency check, thus, you can learn the alarm status on a real-time basis.

- Alarm notification

  You can specify conditions on the alarm console for alarm notification, so that the alarms satisfying the conditions can be forwarded to specified users through wireless Modem or Email.

The [Fault Management System] window is the central user interface for network fault management, as shown in Figure 3-3.

3.2.1 Centralized Fault Management System

The centralized fault management system provides the following functions:

I. Alarm Monitoring, Alarm Browsing and Alarm Query

The system displays alarm information on a real-time basis. You can browse alarm information required by specifying related conditions. The alarms that can be browsed include event alarms and fault alarms.

You may also query alarms by object name, alarm level, alarm name, and/or alarm time.

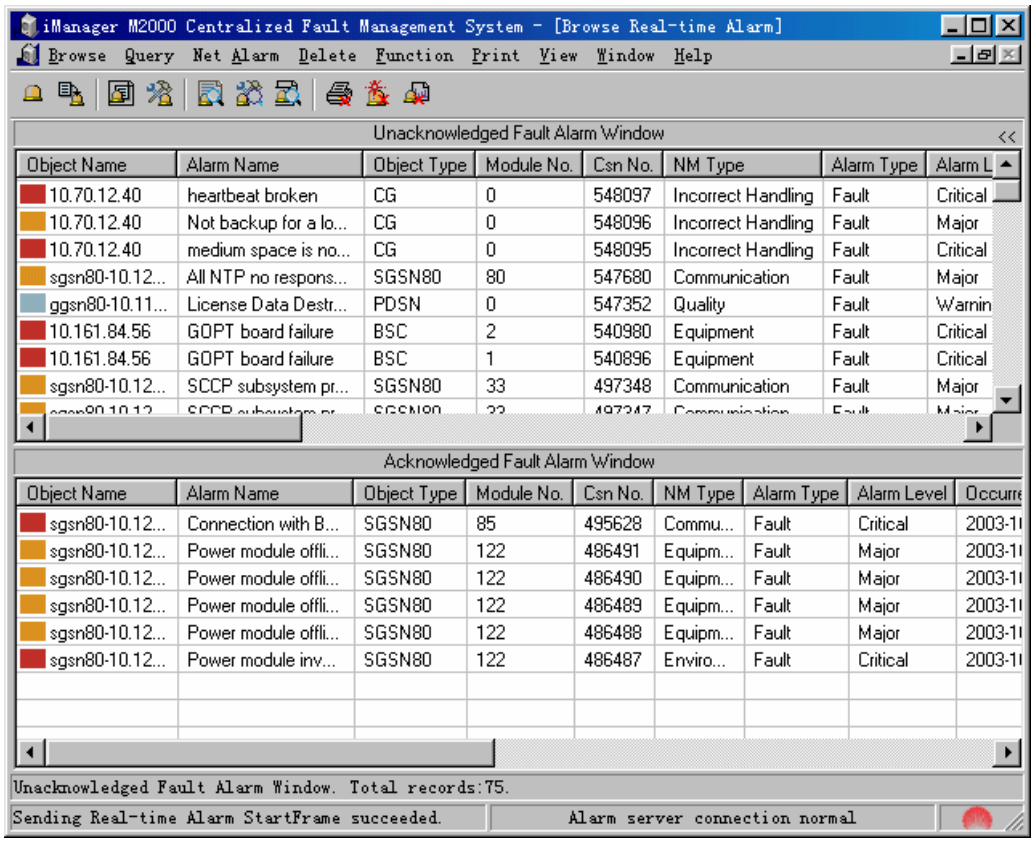

iManager M2000 Centralized Fault Management System - [Browse Real-time Alarm]
Browse Query Net Alarm Delete Function Print View Window Help
Unacknowledged Fault Alarm Window
Object Name | Alarm Name | Object Type | Module No. | Csn No. | NM Type | Alarm Type | Alarm L
10.70.12.40 | heartbeat broken | CG | 0 | 548097 | Incorrect Handling | Fault | Critical
10.70.12.40 | Not backup for a lo... | CG | 0 | 548096 | Incorrect Handling | Fault | Major
10.70.12.40 | medium space is no... | CG | 0 | 548095 | Incorrect Handling | Fault | Critical
sgsn80-10.12... | All NTP no respons... | SGSN80 | 80 | 547680 | Communication | Fault | Major
ggsn80-10.11... | License Data Destr... | PDSN | 0 | 547352 | Quality | Fault | Warnin
10.161.84.56 | GOPT board failure | BSC | 2 | 540980 | Equipment | Fault | Critical
10.161.84.56 | GOPT board failure | BSC | 1 | 540896 | Equipment | Fault | Critical
sgsn80-10.12... | SCCP subsystem pr... | SGSN80 | 33 | 497348 | Communication | Fault | Major
Acknowledged Fault Alarm Window
Object Name | Alarm Name | Object Type | Module No. | Csn No. | NM Type | Alarm Type | Alarm Level | Occurr
sgsn80-10.12... | Connection with B... | SGSN80 | 85 | 495628 | Commu... | Fault | Critical | 2003-1
sgsn80-10.12... | Power module offli... | SGSN80 | 122 | 486491 | Equipm... | Fault | Major | 2003-1
sgsn80-10.12... | Power module offli... | SGSN80 | 122 | 486490 | Equipm... | Fault | Major | 2003-1
sgsn80-10.12... | Power module offli... | SGSN80 | 122 | 486489 | Equipm... | Fault | Major | 2003-1
sgsn80-10.12... | Power module offli... | SGSN80 | 122 | 486488 | Equipm... | Fault | Major | 2003-1
sgsn80-10.12... | Power module inv... | SGSN80 | 122 | 486487 | Enviro... | Fault | Critical | 2003-1
Unacknowledged Fault Alarm Window. Total records:75.
Sending Real-time Alarm StartFrame succeeded.
Alarm server connection normal

Figure 3-3 iManager M2000 centralized fault management system

II. Display of Alarm Information on Topological Diagram

The system shows the NE and link fault status on the vector topological diagram on the real-time basis through alarm indicators of the NE topology icons and the color change of links.

III. Query of Alarms by Board

The system provides a visual operational mode to query alarms by board. Thus, the fault can be located on a specific board. When you query alarms by board, you may also get all alarm information of this board through corresponding operations.

IV. Alarm Prompt

The system provides the alarm prompt function. When an alarm satisfying the preset conditions occurs, the system will notify all Clients and activate the corresponding indicator on the topology map of the system, and drive the alarm box at the same

time. Besides, it can also prompt the alarms that have not been recovered for a long time.

V. Alarm Relativity – Filtering of Repeated Alarms

The continuous existence of certain fault may cause repeated reporting of an alarm. With the repeated alarm filtering, the repeated alarms generated within the preset period, will be stored in the database instead of be shown in the interface. You can set the conditions for repeated alarm filtering as required.

VI. Alarm Relativity – Filtering of Flash Alarms

The flash alarm is an alarm in the "fault-recovered-fault" status all the time. If the flash frequency reaches to a certain degree, an alarm of higher level will be generated by the system automatically and the occurrence times will also be recorded. You can customize the conditions for filtering flash alarms.

VII. Saving History Alarms

The system can keep the data of maximal 500,000 alarm records for as long as 6 months. It also supports the dumping of alarm data, so that you can save the important data to a file of specified format for the convenience of alarm analysis and handling. Besides, you can set alarm field separator to save the alarm records to the file in a defined format.

VIII. Alarm Acknowledgement/De-Acknowledgement

You can confirm the given alarm information which is already known, or cancel the confirmed state of an alarm.

IX. Alarm Statistics

The system can perform real-time statistics of alarms and display the alarm information existing in various NEs. It can also perform statistics of the history alarm information within a certain time period, then display the statistics result in the form of table or chart, or print out the result.

X. Alarm Dispatching List

The system supports the function to print out the alarm in the form of dispatching list (work card). All printed alarms are recorded in the alarm database and can be queried or deleted at any time.

XI. Redefinition of Alarm Levels

The user can define the alarm levels according to the actual requirement.

XII. Alarm Shielding

You can set specified conditions on the NE collection system (Adapter), so that the collected alarms that match with the conditions will be filtered and not sent to the alarm server.

XIII. Alarm Knowledge Database

The alarm knowledge database is used to store the alarm handling experience and methods of users. It can be updated, queried, imported and exported according to the alarm ID and the alarm content.

XIV. Alarm Detailed Explanation Database

The system provides a detailed alarm explanation database to save detailed alarm description is recorded (including the alarm locating and clearing methods). It may guide you to clear faults, and you can perform import/export the data of the database.

XV. Providing Alarm Interface to Third Party

The system can provide alarm-reporting interface to third party, so that the third party can receive the alarm information collected by the iManager M2000 on the real-time basis.

3.2.2 iSmsEmail

Figure 3-4 shows the iManager M2000 SMS-EMAIL Control Terminal.

The iManager M2000 SMS-EMAIL Control Terminal enables the alarms satisfying the preset conditions to be sent to specified users through wireless Modem or Email.

To achieve this purpose, a short message service - Email control program (iSmsEmail) should be installed on the Client PC and the wireless Modem connected to the Client should be set correctly.

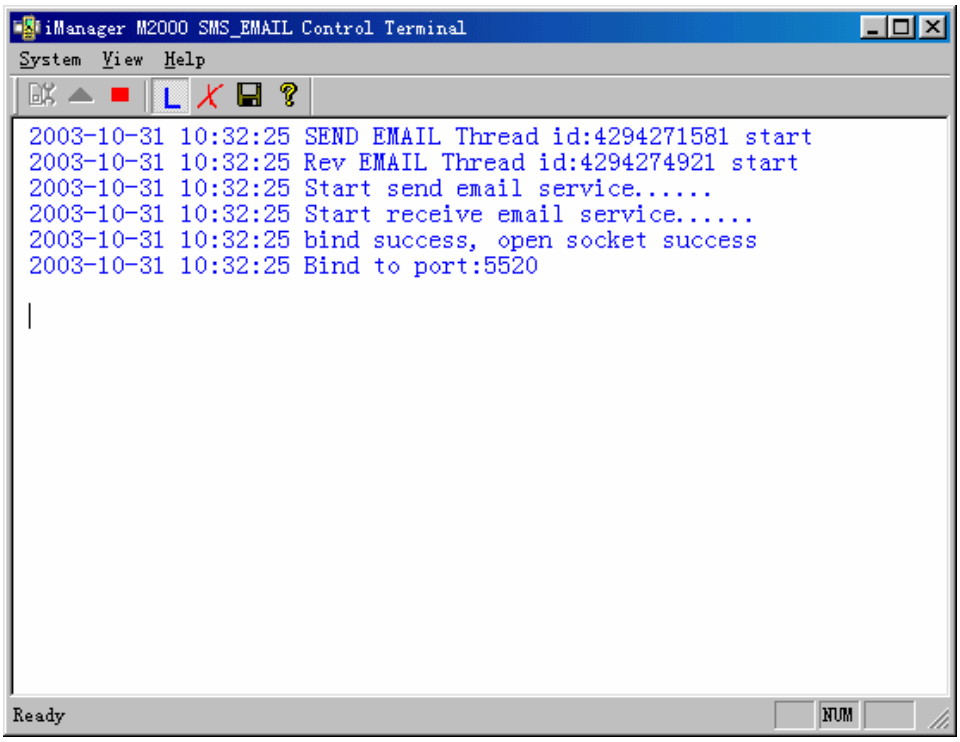

iManager M2000 SMS_EMAIL Control Terminal
System View Help
2003-10-31 10:32:25 SEND EMAIL Thread id:4294271581 start
2003-10-31 10:32:25 Rev EMAIL Thread id:4294274921 start
2003-10-31 10:32:25 Start send email service.....
2003-10-31 10:32:25 Start receive email service.....
2003-10-31 10:32:25 bind success, open socket success
2003-10-31 10:32:25 Bind to port:5520
Ready
NUM

Figure 3-4 iManager M2000 SMS_EMAIL console

3.3 Performance Management

The centralized performance management provides network performance indices, which are valuable to the optimization and maintenance of the entire network.

The iManager M2000 enable the collection and storage of performance and diagnostic data from managed network elements. Some performance data is continuously collected; other performance data and all diagnostic data collection are operator-initiated.

The [Centralized Performance Management System] window is the interface for performance management.

3.3.1 Centralized Performance Management System

The centralized performance management mainly implements the following functions:

I. Display of Performance Items on Topological Map

Important NE performance items can be shown on the topology map of the network management system. You may define the performance item according to actual situation.

II. Registering Performance Measurement Tasks

On a performance console of the iManager M2000, you can configure the performance data of all the NEs to be collected. You can also define a performance measurement task in terms of the measurement items, measurement start time, measurement period, measurement time segment and the days of measurement result reserved.

You may also register a performance measurement task to multiple NEs of the same type.

III. Information and Status Management of Performance Measurement Tasks

You may:

- Query the general information, item information and object information as well as the operating status of all tasks.
- Modify task name, measurement items and measurement objects.
- Change (suspended/activated) the task running status.

IV. Query of Performance Measurement Result

You can query the result data of performance measurement, sequence and print the query results in various modes.

V. Saving Performance Measurement Result

The performance measurement result data can be saved to files in text format or MS Excel format.

VI. Performance Data Storage

After the system collects the performance data, it saves the data automatically into the database table. You can define the number of storage days. The data of up to 1,000,000 records can be saved for more than 6 months.

VII. Statistics of Performance Measurement Results

The system provides statistics of performance measurement result data. It can display the changes of statistics results of the specified objects versus time, and display the distribution of the statistics results in different objects within the specified time. The system can display statistics result in multiple forms, such as histogram, line chart, pie chart, and 3D chart.

VIII. Adaptability to Configuration Modification

You can add measurement objects to a task in operation through the centralized performance management system to meet the requirement of configuration changes. Along with the configuration data modification, the object information in the performance measurement task also changes. In addition, you can also modify the measurement parameters of the suspended tasks.

IX. Setting Performance Alarms

You can enable or disable the performance monitoring to an item of a certain task, and set the upper and lower thresholds of three alarm levels can be set for each item. When the index reaches the upper or lower threshold, an alarm will be generated according to the defined alarm level, so you can learn the system operation condition timely.

X. Self-Defining New Items

You can define new measurement items based on the existing performance items.

3.4 Intelligent Report System

The Intelligent Report System is a set of powerful data mining tools.

With the help of the system, you can:

- Design adequate report templates.
- Extract required data from the specified database.
- Summarize and calculate these data so as to display and output reports.

Based on those reports, you can easily get all data of the service system and then make analysis and decisions.

The iManager M2000 can quickly trace the users' requirement for reports and customize the right report system saving the workload for maintenance personnel in report designing.

The system automatically analyzes all original data and outputs statistics reports on the daily or monthly basis, which minimizes the possibility of data error occurrence caused by manual intervention and makes the data accurate and convincing.

The report server provides the webpage development to the outside and binds the report service program. You can access this webpage through a browser, and perform the installation by downloading the installation package of client software. After the installation, you can log in to the report service program through the client software to obtain the services such as the user management, data source management, report and template management.

I. User Management

The administrator can create or modify users or user groups for the report system, and maintain the user relationship of the system, which is described in detail in the following.

- The administrator can create a series of user group with each user group corresponding to a service (with the **License** file of each service to distinguish the services).
- The administrator can grant the authorities to the user group such as which data source and template can be accessed, and how much can be applied in the access.
- The administrator can create a series of users, each of whom belongs to one or multiple user groups.

When you want to log in to the report system, you should type your ID and password, and select the corresponding working user group.

II. Datasource Management

The administrator needs to write the architecture information of the service database to be dealt into the data source, and designs the report template file based on these data source definitions. Meanwhile, the data source administrator needs to configure the data source information on the basis of the database proxy server installation of the system, and allocate the database proxy servers employed by each data source in the access.

Note:

The information of a data source includes the content as follows:

- The basic information of the data source such as the IP address and the port of the server where the data source is located, type of the database (for example, Oracle and Informix), database name, login ID and password. Using the above information, the system can access the business data.
- The information about the table and stored procedure of the data source.
- Defining which of the proxy programs the system can use to access the data source.

III. Report Management

The report management is similar to the file management, and it aims at managing the report template file, report file and relevant data file.

The design and query of reports involve the database proxy server. You can design the report template file and store it in the home directory of the report service program.

These template files are called in the query, and the service databases are accessed according to the designed content of the template files. Among them, the report service program is responsible for sending and receiving the data, whereas the database proxy server aims at the business data collection.

The report template file includes two parts:

- The format: Defining the appearance of the report, such as the header, footer and heading.
- The data source definition: Defining the tables or the stored procedures of a certain data source to be accessed. These tables and stored procedures will return a result set, which the system employs to generate a report.

The report file is a binary file, which is generated by the system after the template file has obtained the data. Its content includes two parts: format of the report and the data of the report.

Note:

The relevant data information of the management of user, data source and template is stored in the system database.

IV. User-Defining Performance Report

The report template is designed through Report System Client Manager.

Figure 3-5 shows Report System Client Manager.

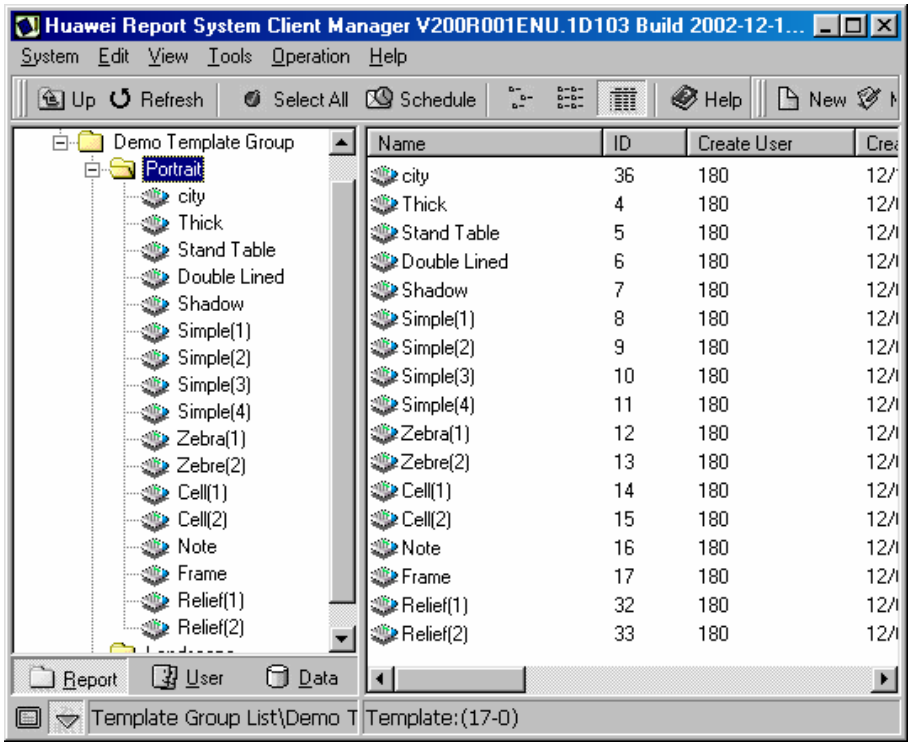
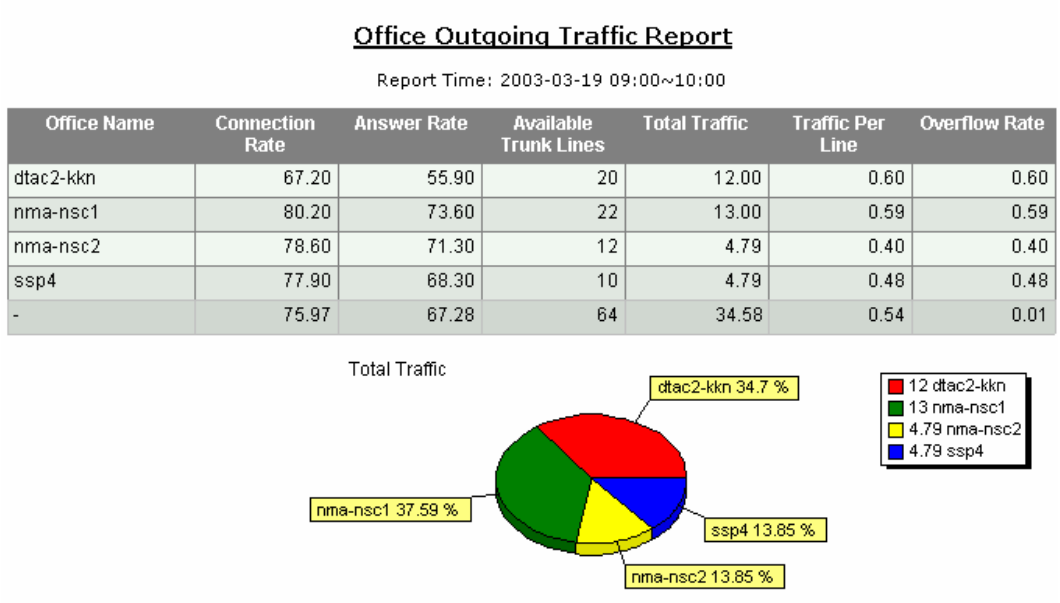


Figure 3-5 Report system window-report template management

The system provides some customizable common or standard report templates, and the users can also create user-defined report templates based on the registered performance measurement tasks.

Figure 3-6 shows an example of user-defined report template, “Office Outgoing Traffic Report”.



Office Outgoing Traffic Report

Report Time: 2003-03-19 09:00~10:00

Office Name	Connection Rate	Answer Rate	Available Trunk Lines	Total Traffic	Traffic Per Line	Overflow Rate
dtac2-kkn	67.20	55.90	20	12.00	0.60	0.60
nma-nsc1	80.20	73.60	22	13.00	0.59	0.59
nma-nsc2	78.60	71.30	12	4.79	0.40	0.40
ssp4	77.90	68.30	10	4.79	0.48	0.48
-	75.97	67.28	64	34.58	0.54	0.01

Figure 3-6 User-defined report

The result data of report can be displayed in bar graph, line graph, column graph, point diagram, or pie chart.

3.5 Common Platform Management

The common platform module involves the topology management, security management and log management.

3.5.1 Topology Management

The [Integrated Network Management System] window is the central user interface for network topology management, as shown in Figure 3-7.

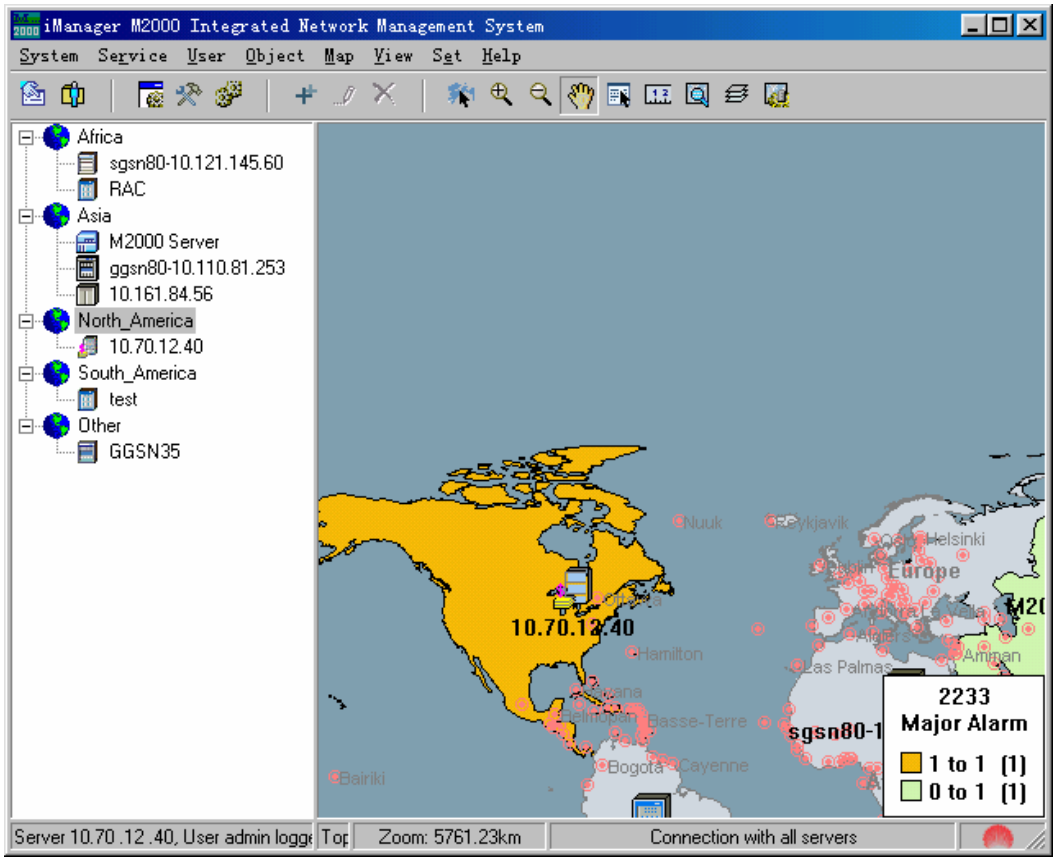


Figure 3-7 Integrated network management system window

The topology management mainly provides the following functions:

I. Displaying the Topological Diagram of the System

The information of NEs, links, office direction, and carriers can be shown through various icons on the topology map of the network. The geographical location information of NEs can also be shown. Meanwhile, the communication status, alarms, and performance items are shown on the map on a real-time basis.

II. Network Navigation

Network navigation is a display mode of topology information different from the topological diagram. Generally in a navigation tree, the NE is shown in the hierarchical relation like "area-NE-link". For example: The NE of BTS is shown in the hierarchy like "area-BSC-BTS".

III. Displaying Virtual NE

The system can display the equipment from other manufacturers on the topological diagram of the network in icons distinguishing from its own NEs, namely display the

virtual icons. This function supports the display of virtual icons only, but not supports the operation and maintenance to the virtual icons. It can help the user get more information of the entire network.

IV. Accurate Positioning of NE

The system supports the interaction of the navigation tree and the topology map. When a NE is selected in the navigation tree, the corresponding NE in the topology map is also selected, and the area it belongs to is shown in the center of the map to ensure the consistency of topology information.

V. Show/Hide of NEs

A certain type of NEs can be shown or hidden according to the actual requirement.

VI. Map Operations

The maps can be zoomed and panned. On the map, the geographical information can be queried. Besides, you can, according to the actual requirement, set the background, delete some shadows or set the display ratio of some shadows, to highlight the local network.

VII. Theme Maps

The system can show the performance items or alarm data on theme maps.

VIII. Visual Operations on Topology Objects

On the topology map, the topology objects can be directly added. These objects can be modified, deleted, or dragged on the corresponding icons. Meanwhile, the system provides the group operation function, that is, multiple topology objects can be selected at the same time for operation.

IX. Diversified Alarm Methods

The system can monitor NE alarms. The NE generating alarms is shown on the topology map by activating the icon indicator. Meanwhile the system supports the function of activating the alarm box tone and transferring alarms to the pager.

X. Activating Single-Point Terminals

Through the NE nodes in the topology map, the system can activate the corresponding single-point terminals so that you can perform operations on the application console, such as NE data configuration, service maintenance, traffic measurement, and bill management.

XI. Subscriber/Interface Tracing

The system provides functions of subscriber tracing, interface tracing and signaling tracing.

3.5.2 Security Management

The [Integrated Network Management System] window is the central user interface for network security management also.

The security management mainly provides the following functions:

I. Subnet Management

You can specify the NEs in related areas to form a subnet, or setup a subnet first, and then add NEs to this subnet. The default entire-network NE of the system is a subnet named "M2000". Super manager with the highest authority will be created automatically. Each subnet can be set with a subnet manager by super manager for NE management.

II. User Account Management

The system allows the manager to add new users. When a new user is added, its information must be specified, including its service authority, login time segment, user password, NEs to be managed, whether to be locked, and so on. The super manager and the entire-network manager can add or delete the account attributes of all users, while the subnet manager only has the authority to add or delete the account attributes of the users in the local subnet.

III. User Login and Logout Management

The system provides an authentication mechanism for user login, thus only the user with valid username and password can log into the iManager M2000 during the specified time segment.

Besides, the user can be log out by himself. However, a logged out user cannot perform any operation unless he logs in again.

If the user does not perform any operation within a certain period, the system will disconnect the connection with him automatically.

IV. Management of User Login to NEs

The system manages the username and password required for NEs access. When the username and password required have changed, the system supports manual modification.

V. System Data Backup and Restoration

Automatic system data backup is provided, including complete automatic backup every Monday and incremental backup everyday. In this way, the data of the previous day can always be restored in the case of system failure. The system also provides the manual backup function. The backup data can be output to external media for storage. In case of system data damage, the data saved by means of automatic backup or manual backup can be used to restore the data back to the status at backup time.

VI. Online User Monitoring

The system monitors the login information and operations of all online users. Any user performing illegal operations can be disconnected by the system by force to guarantee the security.

3.5.3 Log Management

As an important part of the system's security management, the log management provides three kinds of log management mechanisms:

- System log management
- Real-time log monitoring
- Maintenance terminal log management.

I. System Log Management

The system log is the record of startup and shutdown operations of the application console, as well as the operation information concerning common server, configuration server, performance server, alarm server and time server. Through the system log management, you can query, delete and refresh the current log information of the iManager M2000, and get the information of important operation and maintenance already performed in the entire system.

II. Real-Time Log Monitoring

The system monitors the operations of all current login users and records these operations. Thus the manger can monitor the current users and obtain the types of their operations performed.

III. Maintenance Terminal Log Management

The maintenance terminal log records the important operation of the network management system. Through the log management, you can save, clear and refresh the maintenance terminal log, and obtain the detailed information about the important

operations already performed by current terminals on the network management system.

3.6 Online Help

The iManager M2000 system provides detailed online help information, including instructions on system operations and maintenance. It helps you learn the system functions and operations that can be implemented.

The online help modes are very simple and convenient. You can invoke online help through the [Help/Help Topics] in the menu bar. You may also get the help information by pressing <F1> at any time during the operation in a specific dialog box.

3.7 Remote Maintenance Management

The iManager M2000 supports the remote maintenance for the system by means of Modem dial-up. The remote maintenance can implement all functions of the local maintenance. The system can monitor the remote maintenance on the local end, and record the detailed remote maintenance information, including login time, operation procedures, results, exit time, and so on. Any user performing illegal operation can be disconnected by the system by force. When the remote maintenance is completed, the system can output the remote maintenance report.

Chapter 4 Networking Application

According to the NE locations (NEs can be placed in one place or distributed in different places), either local area network (LAN) or wide area network (WAN) networking mode can be adopted.

4.1 LAN Mode

When the iManager M2000 NM is located close to the local terminal of network element, they can be networked through LAN structure, namely, through LAN Switch.

HUB connection mode is shown in Figure 4-1.

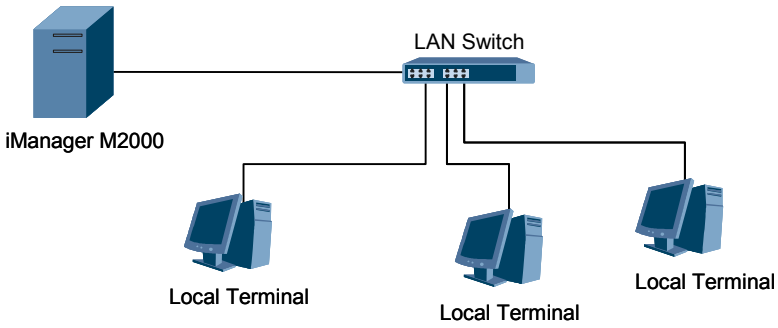


Figure 4-1 HUB Connection Mode

4.2 WAN Mode

When the iManager M2000 NM is located far away from the local terminal of network element, they can be networked through WAN.

As to the composition of a WAN networking, refer to Figure 4-2.

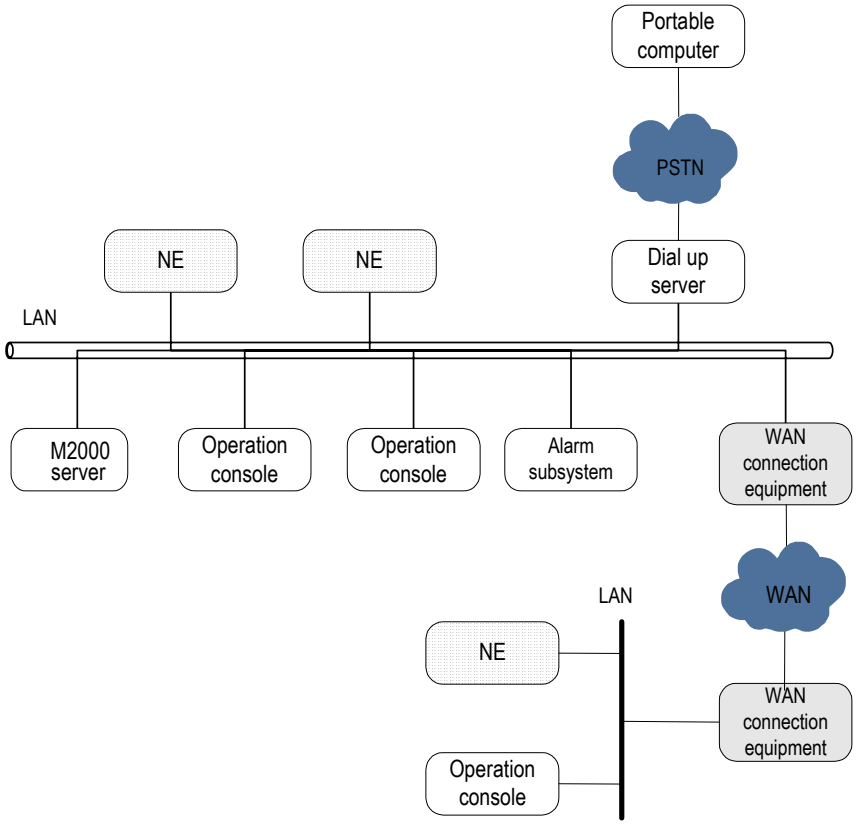


Figure 4-2 Connection of the iManager M2000 system (WAN networking)

E1, T1 and DDN modes are commonly adopted for NM remote management.

If E1 transmission network is available, partial E1 mode will be adopted.

I. Overview of Partial E1 Mode

Figure 4-3 shows the networking of the iManager M2000.

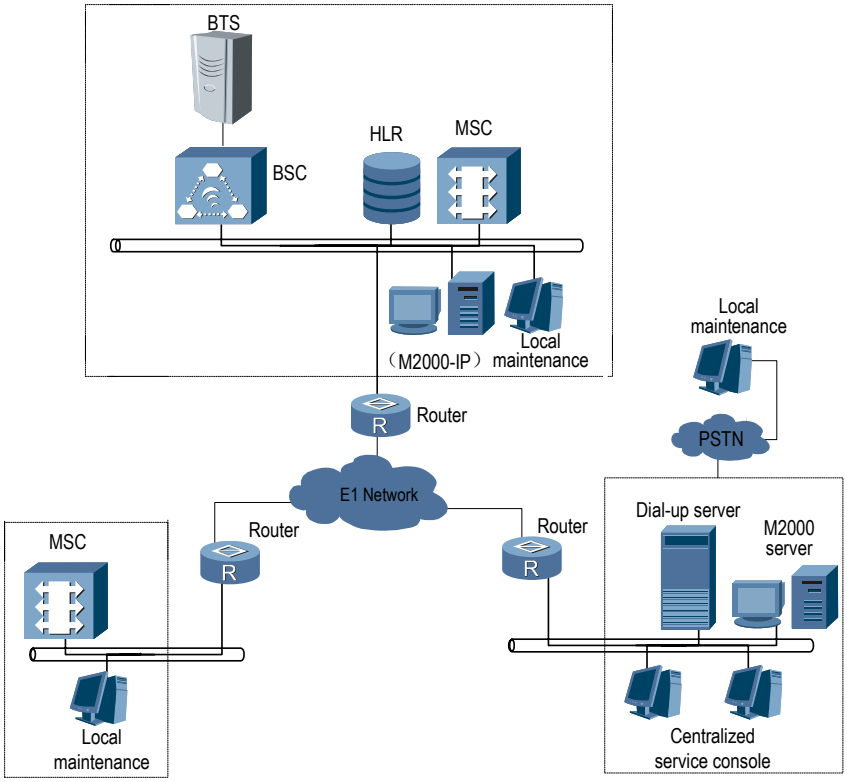


Figure 4-3 Networking of the iManager M2000

The networking of the iManager M2000 does not depend on the transmission mode. Any networking mode, as long as supporting the TCP/IP communication protocol, can be used for the M2000 system. The most popular networking mode is the partial E1 networking mode, which will be detailed in the following paragraphs.

The partial E1 networking mode can be used when there are some E1 lines between two different network segments and these E1 lines have a number of idle timeslots can be used as the transmission bandwidth between the two network segments.

II. Networking Description

Figure 4-4 shows the partial E1 networking.

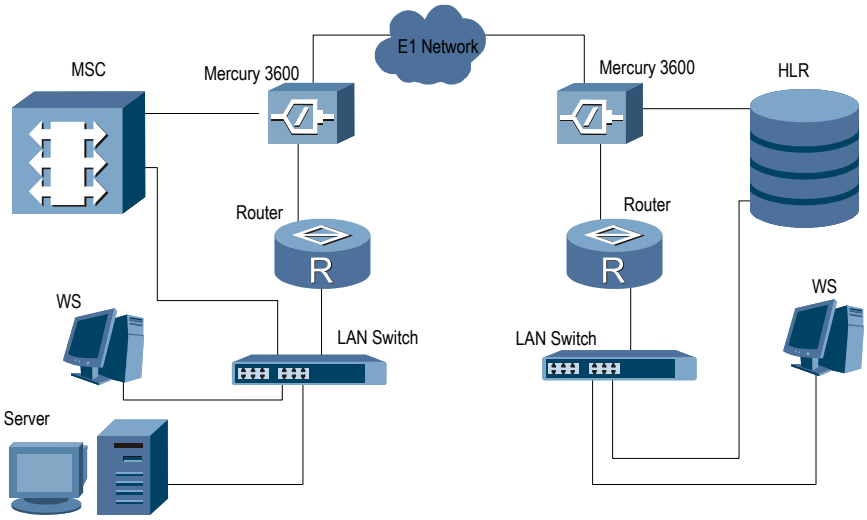


Figure 4-4 Partial E1 networking

Suppose: A set of NM system performs the management of the MSC and the HLR in Figure 4-4. The server and the MSC are in the same field (site), but the HLR is in a different field (site), besides, between the MSC and the HLR there are E1s for signaling transmission.

In this case, a set of timeslot cross-connect equipment (Mercury 3600) can be used to seize the time slots of an E1 (The M2000 data should be allocated with 4 time slots at least, that is, 256K) as the network transmission channel.

III. Features

The partial E1 networking mode is a common networking mode widely used by network operators. Generally these operators have their own transmission equipment, and between the mobile system and the intelligent system there are many E1 lines for signaling transmission. These E1s are only used to transmit signaling but not speech. Among the time slots of one E1, only several can be used as signaling link, the other idle time slots can be used as the transmission channel between WAN network segments.

This mode does not depend on the data office management (DDN/X.25 modes are managed by the data office), so it can make full use of the existing resources, and reduce interface points on such aspects as network address allocation and communication line maintenance.

This solution features many advantages, such as clear interfaces for engineering and routine maintenance, and for convenient fault locating.

Chapter 5 System Reliability

This chapter introduces the protection mechanism of the iManager M2000 system and the reliability measures taken for this system.

5.1 System Protection Mechanism

For each service process and data collection process running in the iManager M2000 system, there is a daemon process. When a service process exits, the daemon process automatically records the exit time. After a waiting period (by default 1 minute), the system activates this service process again to continue the relevant service.

When the system starts to run or the network fails, the system re-synchronizes to get the latest system information so as to ensure that the data is correct and on the real-time basis.

5.2 Reliability Measures

Different reliability measures are taken to ensure the data security and operation security of the iManager M2000 system.

5.2.1 Data Security

I. Backup Policy

Automatic system data backup is provided, including complete automatic backup every Monday and incremental backup every day, so that the data of the previous day can always be restored in the case of system failure. The system also provides the manual backup function. The backup data can be output to external media.

II. Restoration Policy

In the case of system data damage caused by system breakdown or upgrade failure, the automatic backup data or the manual backup data can be used to restore the data to the status at backup time.

III. General Data Transmission

The general data transmission provides the MD5 check mode. The system performs transmission protection and check protection to the transmitted data.

IV. Password Transmission

The system password is encrypted, and then transmitted by means of MD5 check.

5.2.2 Operation Security

I. User Login Management

User login management is implemented through the following two measures:

- Limit for login time segment

  An ordinary user is allocated with a valid login time segment upon creation, so he can only log in the system in this valid time segment.

- Handling of authentication failure

  If the login of a super user fails, the failure information is recorded in the system log and an internal alarm is generated. The super user cannot be locked, but if his login fails for three times, he will have to wait for three seconds every time before next attempt.

  If the login of an ordinary user fails, this user is locked, the failure information is recorded in the system log and an internal alarm is generated at the same time.

II. User Logout Management

If a user does not perform any operation on the terminal within a certain time period, he will be logged out automatically. The automatic logout function can be set. The duration for the automatic logout is 5 minutes by default. Before the use performs any operation on the system next time, he has to log in the system again to get valid user authority through password authentication.

III. Operation Management

The system provides confirmation function for important or global operations.

Note:

The system data are collectively saved at the server, and the high security of the Sybase database system ensures the reliability of the system data.

Chapter 6 System Indices

This chapter provides the technical indices and performance indices of the iManager M2000 system.

6.1 Technical Indices

Technical indices of the iManager M2000 system are reflected by the static value and dynamic value requirements.

6.1.1 Static Value Requirements

I. Number of Manageable NEs for Servers of Different Types

The number of NEs can be managed by the system depends on the performance of the M2000 server. The number of NEs can be managed by different types of servers is listed in Table 6-1. The application server programs can be distributed and run on several servers. One set of the iManager M2000 system can support the distribution of server programs on three servers at most.

Table 6-1 Number of manageable NEs for servers of different types

Server Type	Number of manageable NEs
Sun Blade 150	1 – 5
Sun Netra20 / Sun Blade2000	1 – 15
Sun V880	16 – 30
Sun F4800	31 – 40

II. Storage Capacity and Duration of History Alarm Data

The history alarms can be divided into 4 levels for storage. The max storage volume of each level is 500,000 alarms and the default is 100,000. The max storage duration is 6 months and the default is 1 month.

III. Storage Capacity and Duration of History Performance Data

The performance database supports 2GB data space or larger.

The formula can be used to calculate its performance capacity (Cp):

Cp = 50 + **T** * min (**R**, (**O** * **D**/**K**)) * (270 + **N** * 8))/1M.

T stands for the number of tasks;

R stands for the storage volume of each task, and the default is 860,000

O the number of objects.

D stands for the storage duration.

K stands for the task period.

N stands for the number of items.

The storage volume of each task is restricted by the storage duration selected by the user upon task registration. The max storage volume of history performance data is 1,000,000 records and the max duration is 6 months.

The upper limit for task registration allowed by the system can be modified according to the host performance. The default is:

- The max registration index allowed for a task, that is, 100.
- The max number of objects allowed is 800.
- The max number of tasks the system can store is 200.

With the change of database space, related task data will change accordingly.

IV. Log Storage Volume

300,000 records of history logs can be stored in the system.

V. Data Access of Users

The system can manage 20 subnets and 250 users at most.

6.1.2 Dynamic Value Requirements

I. Responding Speed of Alarm Processing

The normal responding speed is 2 to 3 seconds from the alarm generation on the equipment to the alarm display on the M2000 NM terminal.

II. Number of Alarms Handled by the Alarm Server

Normally the alarm server can handle 200 alarms per seconds at most.

III. Speed of Performance Processing

The normal speed is 1 hour per 36,000 records of performance data.

IV. Speed of the Configuration System Refreshing an NE

The normal speed of the configuration system refreshing an NE is 2 to 15 minutes.

V. CPU Occupancy

The normal CPU occupancy of the system is around 20%.

VI. Technical Indices of Creating Tasks

The system can perform task registration for all items and all measurement objects supported by NEs. Each task allows maximum 100 registered items, supports the measurement period with the smallest granularity as 5 minutes.

When creating tasks, the number of object, item, task and task period of the NE BAM are as follows:

- 300 objects, 20 items, task period: 15 minutes, number of tasks: 30
- 300 objects, 20 items, task period: 30 minutes, number of tasks: 60
- 50 objects, 20 items, task period: 60 minutes, number of tasks: 720
- The rest may be deduced by analogy…

The period from the time the Client modifies tasks to the time the response is received will not exceed 90 seconds.

With the change of performance database space, related task data will change accordingly.

VII. Technical Indices of Deleting Tasks

The Adapter can delete 100 tasks at most each time. The period from the time the Client deletes tasks to the time the response to task deletion is received will not exceed 90 seconds.

VIII. Technical Indices of Activating/Suspending Tasks

The period from the time the Client registers tasks to the time the response to task activation/suspension will not exceed 90 seconds.

IX. Technical Indices of Modifying Objects

New task objects can be measured in the normal mode. The time delay from the time the task object modification succeeds to the time the result is normally reported will

not be longer than 2 periods. The period from the time the Client registers tasks to the time the response to task object modification is received will not exceed 90 seconds.

X. Technical indices of querying task status

The period from the time the Client registers tasks to the time the response to task status is received will not exceed 90 seconds.

XI. Technical Indices of Collecting Results

The system can report the results of 100 tasks. The time delay of complete result report will be no longer than one task measurement period.

6.2 Performance Indices

Performance indices of the iManager M2000 system are reflected by server performance indices, system capacity, and system operation environment indices.

6.2.1 Server Performance Indices

Note:

The following is the configuration of the server Sun F4800:
Minicomputer – Sun F4800 stand-alone server - 4*1.2GHz – 16GB - 2*36GB) - 2*T3 (9*36GB) – -DDS4-Cabinet-English documents – Configuration Table.

System MTBF:	11,353 hours
Total system downtime per year:	6.843587 hour(s)
System availability:	99.921877%
System Mean Time To Repair:	0.5741 hour(s)

6.2.2 System Capacity

To different configurations, the system capacity is shown in Table 6-2, Table 6-3, Table 6-4 and Table 6-5.

Table 6-2 Performance indices of Sun Blade150 in typical configuration

Parameters	System Performance indices
Number of NEs (excluding BTS)	5
Number of online operators	30
Number of data ports	100

Parameters	System Performance indices
Number of managed objects	150,000
Responding time from Server to Client (256K)	Less than 1 minute

Table 6-3 Performance indices of Sun Netra20 in typical configuration

Parameters	System Performance indices
Number of NEs (excluding BTS)	15
Number of online operators	30
Number of data ports	100
Number of managed objects	300,000
Responding time from Server to Client (256K)	Less than 1 minute

Table 6-4 Performance indices of Sun V880 in typical configuration

Parameter	System performance indices
Number of NEs (Excluding BTS)	30
Number of online operators	30
Number of data ports	300
Number of managed objects	900,000
Responding time from Server to Client (256K)	Less than 1 minute

Table 6-5 Performance indices of Sun F4800 in typical configuration

Parameter	System performance indices
Number of NEs (Excluding BTS)	40
Number of online operators	30
Number of data ports	300
Number of managed objects	1200,000
Responding time from Server to Client (256K)	Less than 1 minute

Note:

The following are description for the parameters in the above tables:

The number of NEs is the max number of NEs supported by the system. It does not include the number of BTSs. The number of BTSs is included in the number of managed objects. Maximally 960 BTSs can be accessed to one BSC.

The number of online operators is the number of operators allowed to operate at the same time

The number of data ports is the max number of connections for services which can be accessed to the system at the same time (including such services as centralized performance management, centralized fault management, centralized configuration management).

6.2.3 System Operation Environment

In Table 6-6 is the description of the operation environments of M2000 WSs and servers.

Table 6-6 Operation environments of M2000 WSs and servers

	WS	Server
Hardware platform	P4 -1.7GHz/256MB/40GB or higher	WS - Sun Blade 150/Blade2000
		Minicomputer - Sun F4800
Software platform	English Windows Professional operating system	Operating system: Sun Solaris - 2.8 Database platform: English version - Sybase Adaptive Server 11.9.*X*
Power consumption	300W	Sun Blade 150: 250W
		Sun Blade 2000: 670W
		Sun Netra 20: 680W
		Sun F4800: 3040W
		Sun V880: 1515W
		Router: 40W
Temperature	Nominal working range: 15°C to 35°C (59°F to 95°F)	
	Short-term safe working range: 0°C to 45°C (32°F to 113°F)	
Humidity	Nominal working range: 30% – 65%	
	Short-term safe working range: 10% – 90%	

Chapter 7 Specification Compliance

The iManager M2000 system is in compliance with the following specifications.

7.1 Specifications for General Management

ITU-T M.3010 (1992): Telecommunications Management Network (TMN) Principle

ITU-T M.3400 (1992): Telecommunications Management Network (TMN) Management Functions

ITU-T M.3100 (1992): Telecommunications Management Network (TMN) Information Models

7.2 Specifications for CORBA

MPT (China): NMC-OMC Interface Specification for TDMA GSM Network Management version: 2.0.0 2001

ITU-T: M.3020 TMN Interface Specification Methodology (draft) 1999

ITU-T: X.90x Open Distributed Processing 1997

OMG: The Common Object Request Broker : Architecture and Specification Revision V2.2 1998

OMG: Unified Modeling Language Specification (draft) version 1.3 Jan. 1999

OMG: Common Object Services Specification 1998

OMG: Telecom Event Log Service Oct. 1998

OMG: Notification Service 1998

IETF: RFC 1779 A String Representation of Distinguished Names 1995

ETSI: GSM12.xx Digital cellular telecommunications system (phase 2)

Network Management (NM) 1996

7.3 Specifications for Network Management

ITU-T: M.3100 Generic Network Information Model 1995

ITU-T: X.721 Definition of Management Information 1992

ITU-T: X.733 Alarm Reporting Function 1992

ITU-T: X.736 Security Alarm Reporting Function 1992

ITU-T: Q.821 Alarm Surveillance Function 1993

ITU-T: Q.822 Performance Monitor Function 1994

Appendix A Acronyms and Abbreviations

3GPP2	3rd Generation Partnership Project 2
BAM	Back Administration Modual
BML	Business Management Level
BSC	Base Station Controller
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
CG	Charging Gateway
CORBA	Common Object Request Broker Architecture
EML	Element Management Layer
EMS	Element Management System
GGSN	Gateway GPRS Support Node
GIS	Geographic Information System
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GUI	Graphic User Interface
HLR	Home Location Register
IETF	Internet Engineering Task Force
IIOP	Internet Inter-ORB Protocol
iManager M2000	Integrated Manager Mobile 2000
INMS	Integrated Network Management System
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union--Telecommunication Standard Sector
LAN	Local Area Network
MML	Man Machine Language
MSC	Mobile Switching Center
NE	Network Element
NEL	NE level
NMC	Network Management Center
NML	Network Management Level

NMS	Network Management System
NWS	Network Workstation
OMC	Operation and Maintenance Center
OMG	Object Management Group
PCU	Packet Control Unit
PDSN	Packet Data Serving Node
RAC	Radio Access Controller
RFC	Request For Comments
RWS	Remote Workstation
SGSN	Serving GPRS Support Node
SML	Service Management Level
TCP/IP	Transmission Control Protocol /Internet Protocol
TMN	Telecommunications Management Network
WAN	Wide Area Network